

White paper

The New Digital Perimeter is the Individual



Content	
Abstract	2
Employees need to be creative without being constrained	2
Challenges managing the transition to a modern digital workspace	2
Yesterday's solution is not today's answer	3
Different is the new normal	5
How Citrix and Fujitsu deliver a modern digital workspace	6

Abstract

As businesses of all kinds become digital, organizations depend on the ability to create new disruptive business models, new ways to engage employees and customers, and new ways to work. Yet, the complexity and limitations of legacy systems and concerns over security are hindering enterprises from moving fully into the digital future.

To realize the agility of cloud without complexity and security slowing you down, you need the flexibility and control of digital workspaces. Citrix Workspace integrates diverse technologies, platforms, devices, and clouds, so it's flexible and easy to deploy and enabling new technology without disrupting your existing infrastructure. IT and users can co-create a context-aware, software-defined perimeter that protects and proactively addresses security threats across today's distributed, multi-device, hybrid- and multi-cloud environments. Unified, contextual, and secure, Citrix and Fujitsu work together in building the workspace of the future today, so you can operationalize the technology you need to drive business forward.

Employees need to be creative without being constrained

Employees working productively during set traditional business hours, in fixed locations and on a single company owned device is quickly becoming a thing of the past. While at the same time the security, governance, monitoring and management of sensitive apps and data is becoming even more multifaceted. Adopting a secure digital Workspace enables both worlds to grow and succeed together.

Previously, employees started their days at nine o'clock Monday morning. They worked within a beige cubicle, leaving only to grab a coffee, cigarette or attend meetings armed with their corporate tagged laptop. And at the end of the day they logged off of that laptop, turned off their fluorescent lamp and commuted back home where they changed their persona from "employee" to Mother, Wife, Husband, Daughter, etc.

But as business relies less and less on in house, static applications and more on internet and cloud based technology those definitions become more and more obsolete. The browser replaces the desktop for many productivity solutions, and the constraints of the cubicle are shattered. Now, a workspace is not defined by a building but by the individual's behavior at any given location, time and on any device. The digital perimeter extends beyond the glass revolving doors of the office building and has to be able to follow the employee wherever they need to go.

SaaS applications have contributed to today's work-from anywhere culture, giving workers the ability to access their workspaces from almost any device. With fewer ties to a physical location, employees can:

- Be productive from anywhere with an internet connection.
- Use their favorite devices, whether desktop computer, laptop, tablet, or smartphone.
- Pull up key documents in important meetings, no matter where they're held.

But the new way employees' access their workspace has also created a host of problems for users, managers, and IT teams alike.

Challenges managing the transition to a modern digital workspace

With this new evolution of "work from anywhere" corporate IT is faced with a growing list of challenges the likes of which they may not have seen since the switch from typewriter to personal computer.

Security

Individual SaaS applications often come with individual security and compliance policies, data management, and access management. The results are multiple security perimeters and styles, which is difficult, if not impossible, for IT to fully govern.

Access

A lack of oversight across applications prevents IT's ability to limit or allow access to sensitive data based on unsecure devices, locations, or networks.

- Example: An employee leaves their personal device on the city bus as they travel to their child's doctor appointment. That employee is able to access sensitive apps and data when they return to the office and use a corporate owned device. However, at the same time Bob the Burglar is able to access the same apps and data from the rogue device.

Authentication

Employees can't simply start their day. With multiple applications comes multiple logins, interrupted workflows and stifled productivity. And with so many usernames and passwords to remember, it encourages bad password habits such as using the same login for multiple accounts or writing them down. And multiple logins mean that IT can't simply create or remove global access easily.

- Example: In order to become effective and start using a particular SaaS application, employees need to authenticate multiple times and with disparate passwords for each service. To overcome this blocker, the employee writes their passwords in a text file on their desktop.

Integration

With employees completing multiple processes in different applications, workflows are fragmented and processes are often redundant. Finance might use one application for expenses and another for reimbursements, without a process and workflow to keep the two in sync.

- Example: An employee inadvertently submits a duplicate expense report. Because the Finance team lacks integration between applications, the employee is paid twice for a careless oversight.

User Experience

Applications are often optimized for different browsers, devices, or operating systems, leaving employees with an inconsistent user experiences. And with little to no oversight capabilities, IT teams can't solve for a variety of issues. This also often limits the range of devices that employees can use for unique or special-purpose applications.

- Example: An employee is accustomed to using application X through a traditional Windows interface or browser. When they turn to their tablet or mobile device to access the same application, they are presented an interface that is optimized for that form factor, throwing the employee into an unproductive tailspin and generating a help desk ticket.

Analytics

Disconnected (or non-existent) analytics for individual apps don't give IT administrators the full view of usage, compliance, and security profiles. IT is ultimately unable to gain actionable insights to manage or control the user environment.

Governance

Without a single place to configure and monitor SaaS applications, IT can't properly manage data across an organization, leaving them unable to improve or automate process across apps.

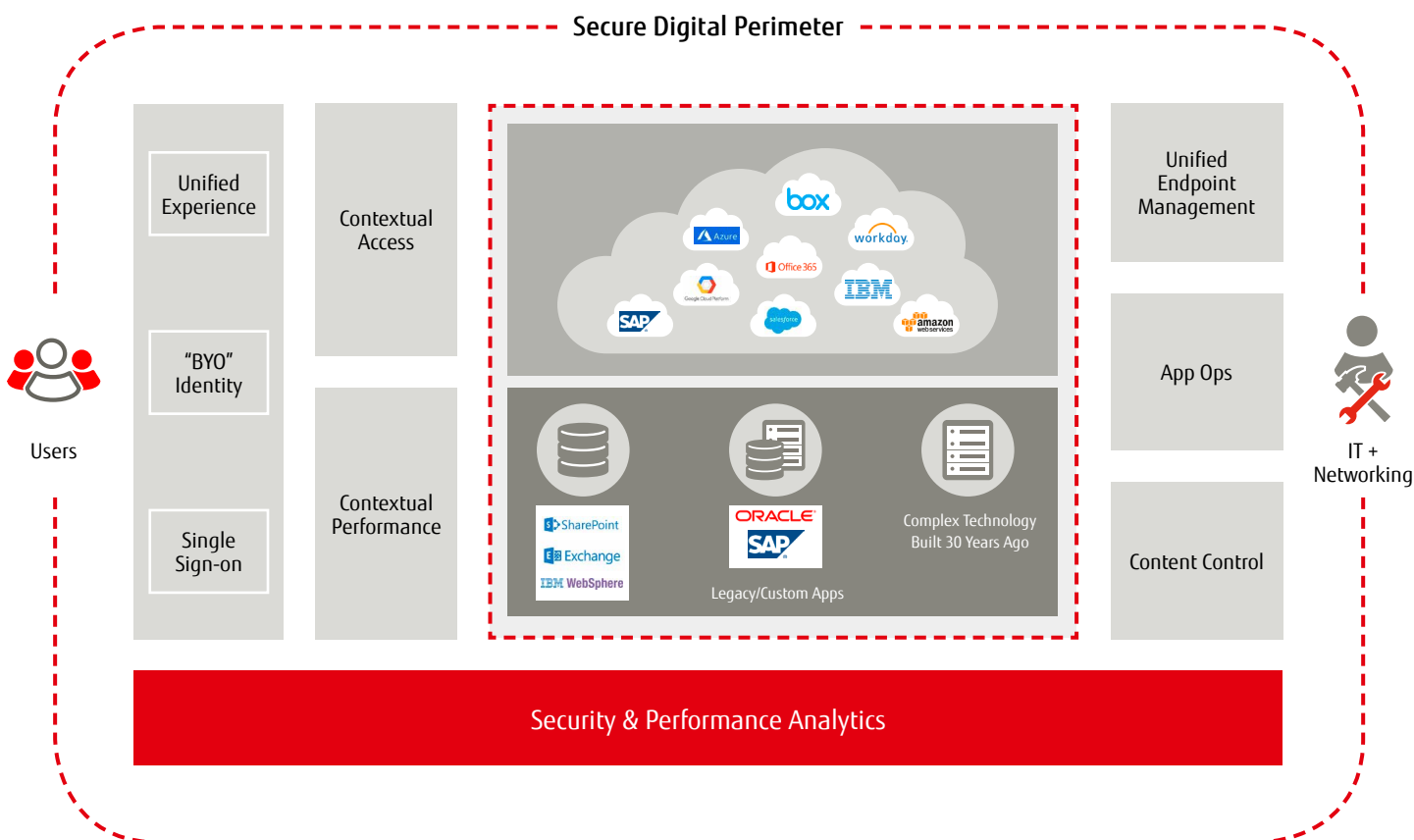
Data Management

With multiple cloud applications, there's no way for IT to know or audit where data is stored or how it is being managed and shared.

Yesterday's solution is not today's answer

There was a time when corporate IT would block access to these SaaS applications and even employee owned devices with a blunt and simple "no". This approach is not acceptable today and not what employees or the business expect from their technology teams. In fact, a result of IT employing blocking tactics is that employees will turn to "shadow IT" by using solutions that they choose and purchase without IT control. By delivering a secure digital workspace, these modern concerns can be solved while disparate applications, content and services are provided and true value is delivered to the business. Citrix has evolved its portfolio to simplify how a secure digital workspace can be provided.

Citrix Secure Digital Workspace



This portfolio offers the following major customer benefits:

■ **Unified experience**

No matter what application or data is paired with what device, getting access to that content is intuitive and consistent, simplifying the experience for the user.

■ **“BYO” Identity**

Identity is the key to entitlement and more than just a set of credentials. IT can utilize their existing cloud-based identity provider to feed into contextual control of the digital workspace.

■ **Single sign-on**

SSO lets users log in once and then access all of their in-house or cloud hosted applications without further logins, simplifying user experience and reducing the likelihood of insecure bad password habits.

■ **Contextual access**

With more granular insight into identity and, devices, IT are now able to have an adaptive approach to creating “software-defined perimeter,” automatically tailored security and rights are applied to an individual in a contextual manner, based on devices, networks, locations, and behavior.

■ **Contextual performance**

Dependent on user, device network and application needs, the appropriate method of application delivery can be provided to a user and application functionality automatically adapted to device features, optimizing the user’s experience and therefore increasing their productivity.

■ **Unified Endpoint Management (UEM)**

UEM allows IT to manage PCs including desktops and laptops, mobile devices and IoT devices more seamlessly. It combines Enterprise Mobility Management (EMM) with traditional client management tools such as System Center and IoT management capabilities. This combined set of capabilities gives a single point of control and insights from the vast variety of devices now utilized in many organizations.

■ **App Ops**

Managing your applications through an application layering service enables the optimization of release and monitoring operations to support better alignment with new operating system update lifecycles and rapid application onboarding demands.

■ **Content Control**

Security around data at a file or device level, whilst providing a logical integration between users or applications through customizable workflows and a stateful application environment. Intuitive and simple controls make it easy for IT and users to apply appropriate protection without compromising experience or collaboration.

■ **Centralized analytics**

IT teams won’t have to go into multiple applications to gather analytics and attempt to compare them across different metrics. Instead, they can use the consolidated information across applications, networks, content repositories to provide actionable insights for the organization and provide granularity to Contextual Access and Content Control.

■ **Governance in IT’s hands**

With a single control panel across applications, data and networks, IT can easily manage data across the organization.

Different is the new normal

Most organizations would say they are on a journey to the cloud, yet each of their journeys will be unique.

The common goal would be the flexibility to adopt the cloud services they want, when they want; the freedom to use any combination of on-premises and cloud resources from any vendor; and simple ways to activate, secure, manage and optimize diverse applications and services so that the entire cloud journey delivers the best results for their users and business.

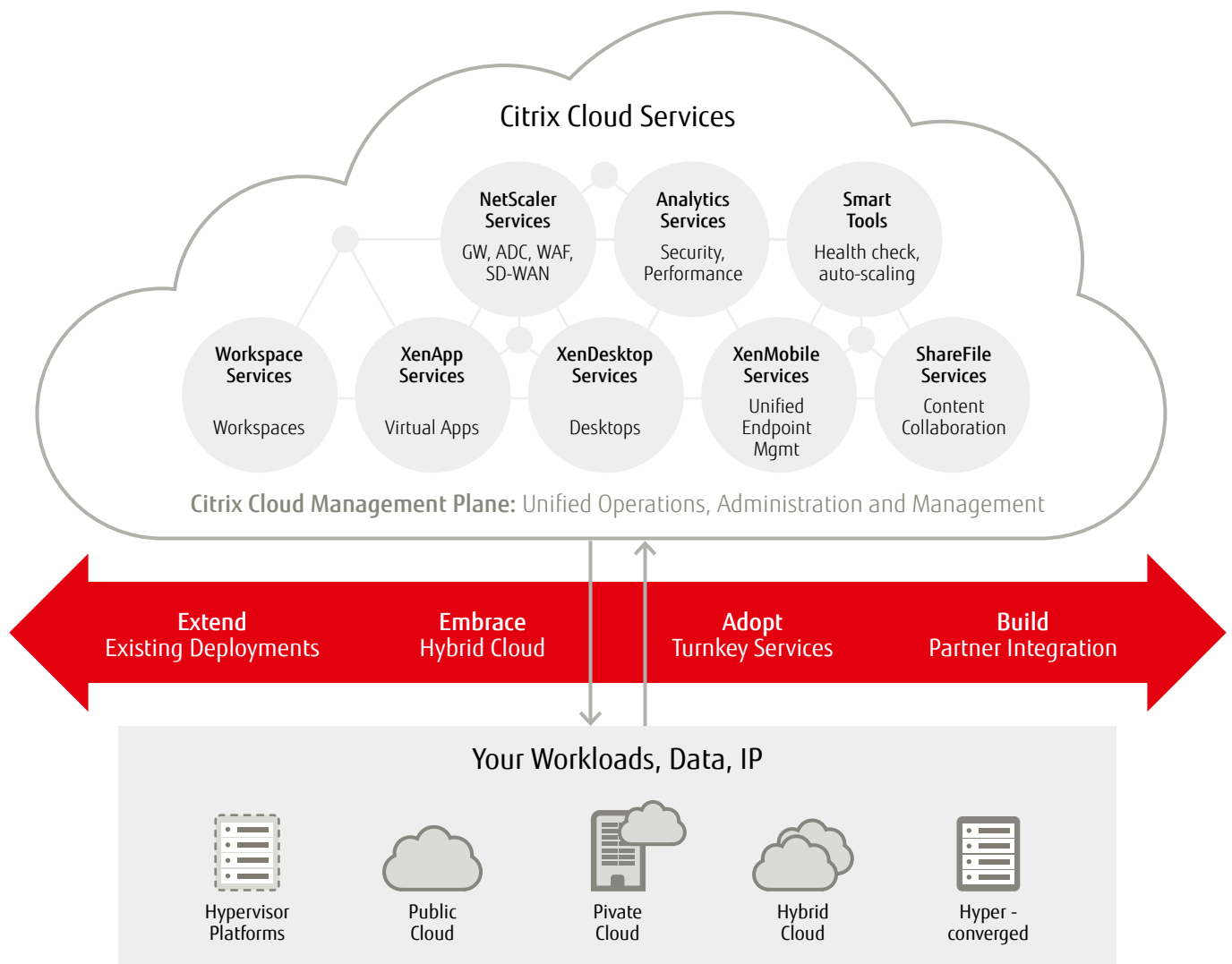
Citrix Workspace and Citrix Cloud solve the challenges of this complex scenario by taking a unique hybrid approach to managing and aggregating resources and services.

Citrix Cloud is a platform for hosting a portfolio of Citrix Cloud Services. While the control plane for these services resides in Citrix Cloud and is provided and managed by Citrix, they enable the actual resources for virtual apps and desktops, mobility, secure access control and content collaboration to be hosted and executed wherever the customer chooses. Citrix Cloud Services are not mandatory for deploying Citrix app, desktop or mobility solutions, but do include services such as

Smart Tools and Analytics Service which add value and extend the functionality for new or existing deployments following traditional on-premises architecture.

Whether you subscribe to one or many Citrix Cloud Services, there is a single point to manage their configuration, ensuring simplicity in the form of a consistent user interface, a single console for administration, services integration, and SaaS-style upgrades to all services. This cloud service also enables deployment of certain environments into whatever infrastructure you desire or define. ANY infrastructure, ANY hypervisor, ANY cloud, allowing organizations to define where the workloads, data, IP to reside, giving choice of where to deploy to better manage compliance, security, and data sovereignty issues.

This refreshed, secured and flexible approach allows complete freedom to mix resources hosted on-premises with those in a cloud, and manage multiple geographic locations enabling the management and control of those workloads across a hybrid, multi-cloud environment, with a single management plane. In turn employees are provided with a unified, secure and reliable access to all the apps and content, they need to be engaged and productive anywhere, anytime.



How Citrix and Fujitsu deliver a modern digital workspace

With over 20 years of strategic partnership, Citrix and Fujitsu offer a comprehensive collection of solutions and services to deliver a complete digital workspace. Our joint installed base covers over 4,000 private and public organizations around the world, including many of the world's largest Citrix Workspace deployments of desktop virtualization and managed mobility services. Delivered on-premises, off-premises or from the cloud, the sheer breadth of the portfolio gives you unprecedented choice to find a tailored workspace solution that exactly fits to your organization's needs. With one-stop shopping for the entire Citrix Workspace and Citrix Cloud portfolio, Fujitsu provides you with the fastest on-ramp to a modern secure digital workspace.

Citrix and Fujitsu share a close relationship with Microsoft, the clear leader in employee productivity solutions and enterprise cloud. This in turn with the fact that Citrix hold the market lead in virtualized end user computing, and Fujitsu being a leader in managed workplace services, means together the three organizations are best placed to accelerate any 'Fit for Digital' initiative within enterprises.

Fujitsu solutions for Citrix Secure Digital Workspace environments:

■ Fujitsu data center systems

Fujitsu data center systems featuring all-flash storage, hyper-converged systems and server-side graphics processing provide a high-performing platform for Citrix workspace environments. With an excellent price / performance ratio, Fujitsu x86 servers provide the most powerful virtualization platform. And with tailor-made Fujitsu integrated systems featuring market-leading virtualization technology, we reduce complexity, time, risk and cost in deploying the infrastructure foundation to provide you with fastest time to production for your Citrix workspace, desktop, app or mobility solution.

■ Fujitsu client systems

With a broad range of flexible, secure and reliable stationary and mobile devices certified for Citrix virtualization technologies, Fujitsu client systems meet every user requirement. Fujitsu thin client systems provide integrated security features supporting SmartCards or biometrics like Fujitsu's patented palm vein scanning technology, enabling multi-factor authentication. In addition, lean and customizable operating system support in combination with best-in-class client management provides an operating platform that is used for the largest thin client deployment world-wide with over 200,000 devices.

■ Fujitsu services

As part of the broader digital workplace services offering Fujitsu provides managed end user virtualization services based on Citrix technology including virtual desktop infrastructure, virtual desktop as a service, hosted shared desktops, and applications all delivered via public, private or hybrid cloud infrastructures. These services are complemented by professional services, infrastructure support services, financial services and security services provided by Fujitsu or its local partners. Fujitsu's global service capabilities are available both on-shore and off-shore from 5 global delivery centers and local service desks in more than 70 countries. Nearly 700 Fujitsu employees hold Citrix technical certifications, more than any other system integrator. You profit from the experience of a global service provider managing over 5 million desktops worldwide making Fujitsu a leader in the Gartner Magic Quadrant for Managed Workplace Services.

Joint customer case studies

Fujitsu has successfully delivered many Citrix virtual desktop projects across various industries:

- For Statistics New Zealand, Fujitsu deployed a Government Desktop-as-a-Service solution enabling secure access to critical applications for thousands of users, and real-time data collection.
- As part of a workplace enablement initiative, Fujitsu helped Royal Bank of Scotland to extend its virtual desktop environment from 20,000 to 90,000 users.
- For Carea, a social and health services provider from Finland, Fujitsu deployed a Citrix-based virtual client services solution that makes each of the 1,600 users' desktops available remotely and introduces the ability to transfer a single session on the move.
- For the Danish Municipality of Halsnæs, Fujitsu deployed a Citrix-based virtual desktop environment serving around 1,600 active users from across the municipality's administrative services.
- King Fahad Medical City (KFMC), the largest and most advanced medical complex in the Middle East situated in the heart of Riyadh City, worked together with Citrix and Fujitsu to replace its PC infrastructure with a virtualized desktop infrastructure.