Deliver a cloud strategy that works for your business — and your workforce

Use an integrated, cloud-hosted digital workspace to make users more productive, simplify IT, and ensure the security and agility your business demands
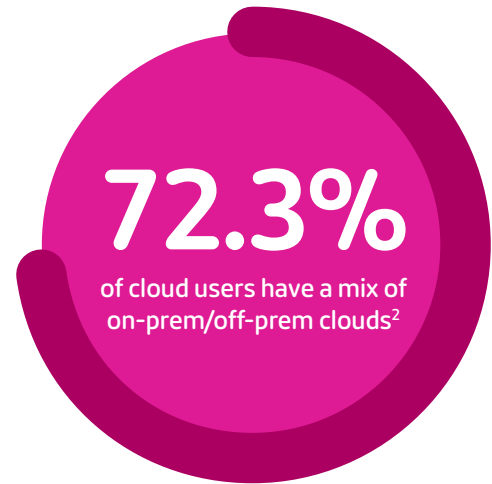
Contents

Introduction

There have never been so many ways for people to get work done. Mobile devices and apps let employees become productive anywhere, at any time. That's great for the business—but it complicates life for IT.

We've introduced SaaS, cloud, and mobility, but people still rely on Windows desktop apps, web apps, and virtual apps. Companies are moving workloads and apps to the cloud, but most will continue to use on-premises resources as well for the foreseeable future.

The more options people have, and the more diverse the enterprise environment grows, the more difficult it becomes for IT to secure, provision, patch, update, repair, and maintain all the software and hardware now in use across the workforce.

It can be tempting to view this as growing pains on the road to the cloud—once you consolidate everything on a single cloud platform, all this complexity will vanish. Hybrid and multi-cloud IT is likely here to stay, and that's a good thing. We just need an effective way to manage the resulting complexity.

73%
of organizations have at least one application or a portion of computing infrastructure in the cloud[1]

72.3%
of cloud users have a mix of on-prem/off-prem clouds[2]

How to get IT simplification right

As their environment grows more diverse, overwhelmed IT organizations often turn to point solutions to address specific areas of need such as unified endpoint management (UEM), virtual app delivery, enterprise mobility management (EMM), network security, identity management, file sharing and content collaboration, application delivery, cloud security, and so on. But proliferating tools just add complexity, not to mention cost, and management becomes even more challenging.

Meanwhile, the more IT struggles to manage this complexity, the greater the chance of gaps in security and compliance, performance problems, business continuity issues, and other fires to fight. Having hoped to gain new agility in the cloud, the company instead finds itself bogged down by siloed technologies, piecemeal management, and a frustrating, disjointed user experience.

Point solutions are no solution to rising complexity. To deliver all the apps needed by today's dynamic, mobile workforce without drowning in unintended consequences, companies should turn instead to an integrated, cloud-hosted, secure digital workspace.

With a secure digital workspace, you can:

• Deliver a coherent, seamless, and engaging experience for employees
• Simplify IT management and reduce its cost
• Take a holistic approach to security and compliance while closing gaps
• Help the business maintain peak agility

83%
of organizations say complexity of their organizational structures and IT infrastructure puts them at even greater risk for security breaches.[3]
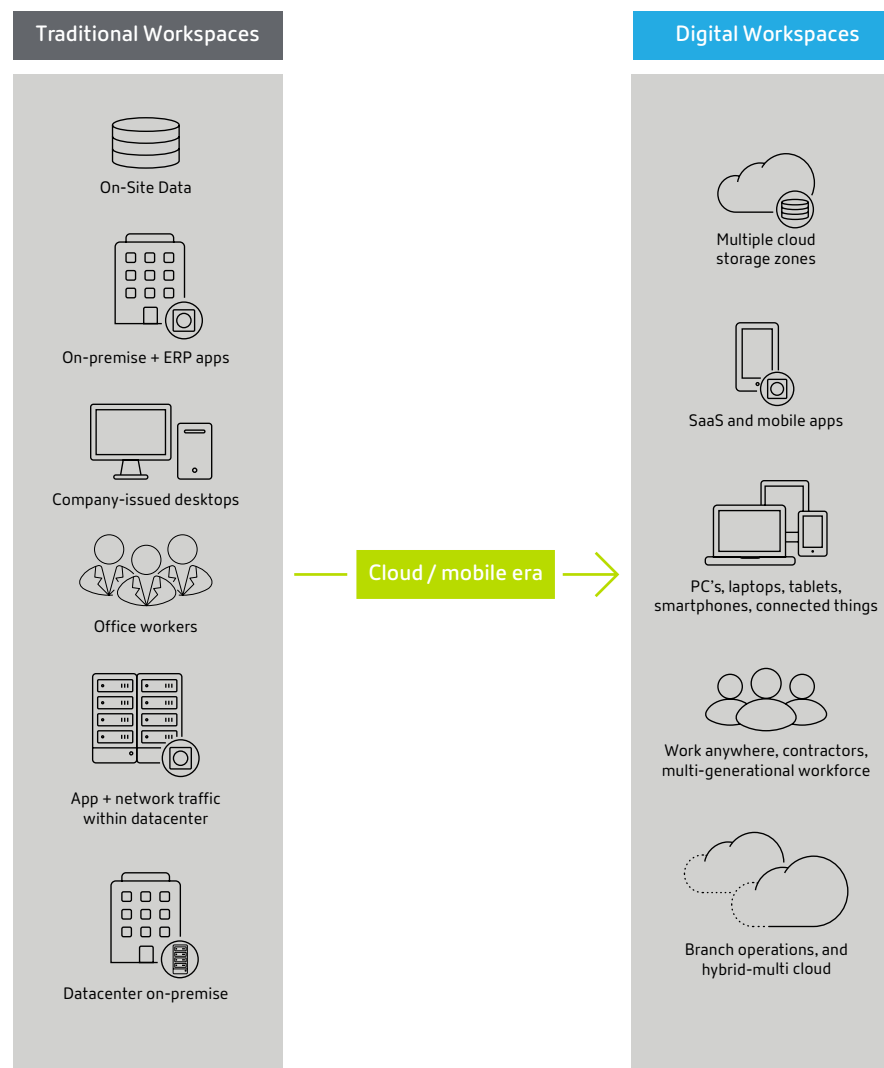
Niche products = complexity
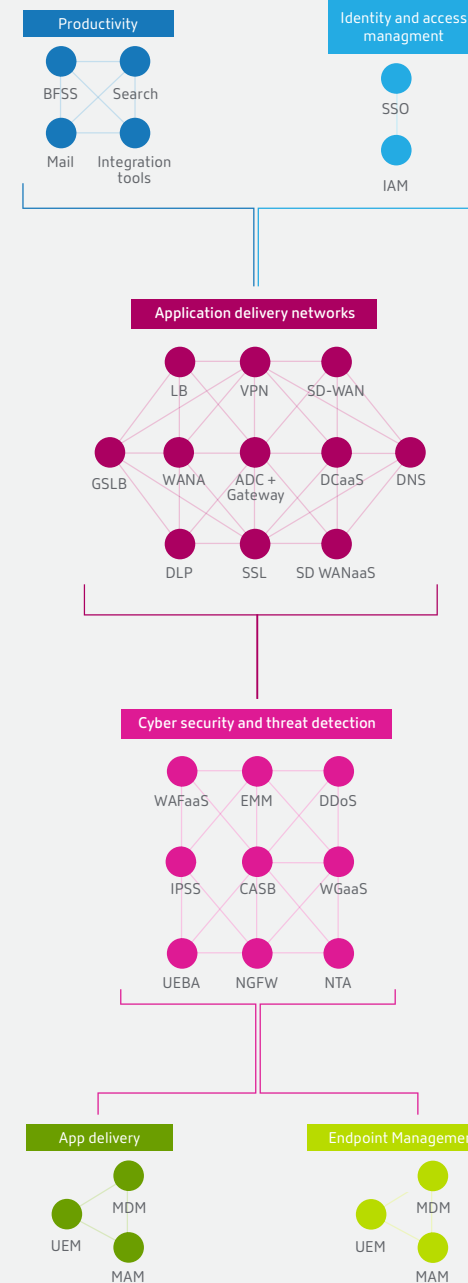
Making both work and IT simpler with a secure digital workspace

A digital workspace provides a single place for people to securely access all their apps, desktops, and data from anywhere. Employees get a consistent single sign-on experience no matter how or where they work, including:

- Any device
- Any cloud
- Any network
- Any type of app—cloud/SaaS, web, mobile, Windows

On the back end, IT gets unified security and control without the cost and complexity of myriad point solutions. Complementary technologies including device security, secure file sync and sharing, network security, and intelligent analytics help strengthen security, while user-based analytics highlight potential risks and areas for operational improvement.

Traditional Workspaces

On-Site Data

On-premise + ERP apps

Company-issued desktops

Office workers

App + network traffic within datacenter

Datacenter on-premise

Cloud / mobile era →

Digital Workspaces

Multiple cloud storage zones

SaaS and mobile apps

PC's, laptops, tablets, smartphones, connected things

Work anywhere, contractors, multi-generational workforce

Branch operations, and hybrid-multi cloud
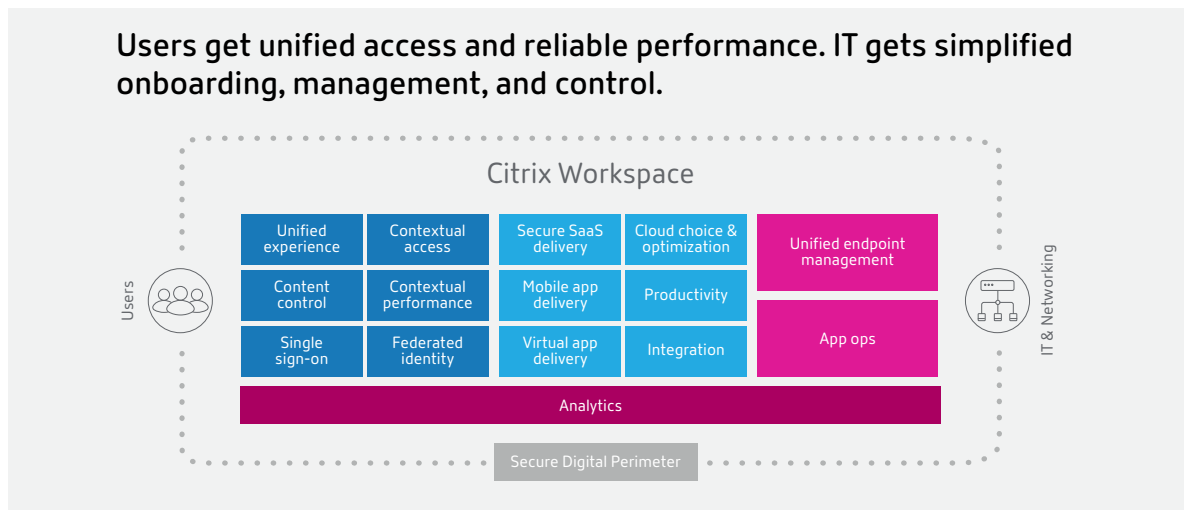
Make a safer, smarter move to the cloud

Security is always a concern for companies moving workloads to the cloud or using SaaS or web apps. Going beyond the data center can seem like a loss of control—and it often is.

A secure digital workspace keeps companies in control. IT gains a single place to monitor and control access to all the cloud services people use—even unsanctioned apps they've found on their own. Controls like watermarking, blacklists and whitelists for URL categories and specific websites, and the ability to constrain copy/paste and download functionality help IT manage risk effectively. A secure browser within the workspace protects people who've inadvertently clicked an unsafe link in a document or within an app such as Salesforce. Data can be encrypted and secured wherever it is— stored on a device, in the cloud, or in transit. App-layer security and firewalls for web apps and services deter zero-day exploits and DDoS attacks.

Beyond reducing the risk of cloud service adoption, a secure digital workspace also helps IT ensure that its budget is being spent in the best possible way. Unified visibility, data, and analytics on the resources people use most—and how they perform—help companies make smarter investment decisions and better use of business technology resources.

82%
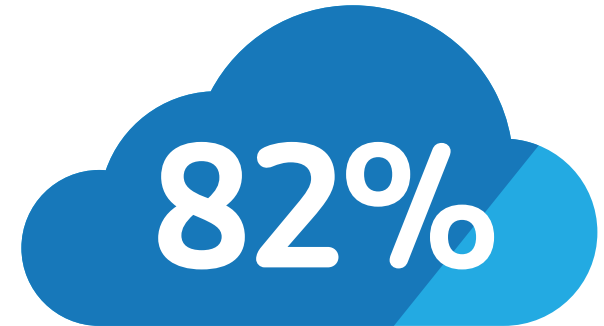
believe their organization's ability to migrate apps to the cloud is hindered by the increased complexity of their network infrastructure[2]

Users get unified access and reliable performance. IT gets simplified onboarding, management, and control.

Citrix Workspace

Users	Unified experience	Contextual access	Secure SaaS delivery	Cloud choice & optimization	Unified endpoint management	IT & Networking
Content control	Contextual performance	Mobile app delivery	Productivity
Single sign-on	Federated identity	Virtual app delivery	Integration	App ops
Analytics

Secure Digital Perimeter

Help people become more productive and engaged

It's hard for people to get work done when they have to deal with a different authentication process for every resource they access, or change the way they do things based on the type of device or app they're using.

With a secure digital workspace, IT can give employees a seamless experience regardless of the type of device they use, including:
- Single sign-on to all their apps, of any type, accessed through a single URL
- Session roaming so people can open an app on one device, then resume work on a different device and pick up exactly where they left off
- A single place for people to find and access all their files, whether they're on corporate file servers, Microsoft SharePoint, or public or private file storage, using any device

Making it easier for people to get work done is obviously good for the business. So is having a more empowered, engaged, and satisfied workforce. When people have the tools they need to do their best work, the whole organization becomes more inspired, innovative, and productive. The company also becomes more attractive to top talent—people want to work there, and they stay there longer. This is a powerful advantage in an industry with high turnover and fierce competition for the best employees.

Companies with engaged employees outperform those without by

202%[4]
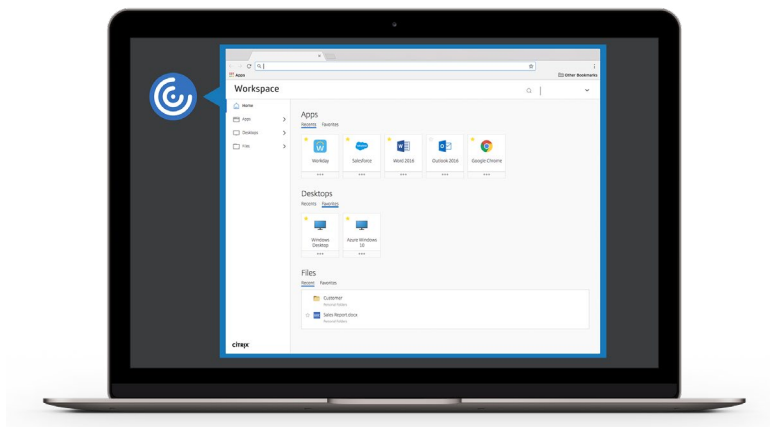
Simplify endpoint management and security

With so many PCs, laptops, smartphones, tablets, and IoT devices in the enterprise environment, IT admins can feel like they're always logging into one device management console after another. This wastes time and makes it hard to maintain consistency in policy enforcement—especially when different groups manage different types of endpoints. And the diversity of devices will only grow as IoT continues to evolve.

A secure digital workspace simplifies endpoint management by letting you use a single console to apply a common policy framework across resources, regardless of the type of device, app, operation system, or network. Admins gain complete visibility and control over user access, helping them protect SaaS, web, and mobile apps as well as content no matter where or how they're used.

6.58

In 2020, the number of network-connected devices per person is expected to be 6.58, resulting in about

50 billion
connected devices in total[5]
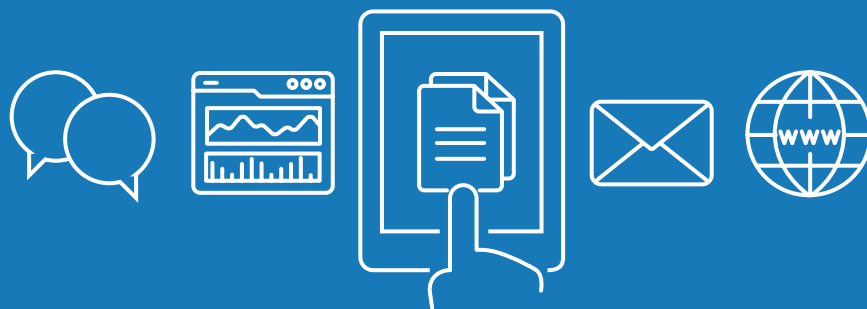
Increase business agility

Traditional processes for onboarding employees and opening branch offices are a model of inefficiency. Admins create images of a standard, approved desktop with the appropriate apps, download the image onto the desktop or laptop, and then either wait for the employee to physically pick it up at the office, or else pack and ship it to them. Future app updates follow a similar process. This time-consuming, labor-intensive approach delays the impact of key hires and strategic initiatives.

With a secure digital workspace, employees can buy any type of device they want and simply log into the company network to be automatically provisioned with corporate-approved apps pre-configured with the right security controls. Able to expand and grow more efficiently and securely, the company can realize the improved business agility promised the cloud.

Ensure business continuity

Responding to a disaster (natural, IT, cyber, civic) can be a slow and messy process. If your strategy depends on procuring and configuring more PCs, and then distributing them to users unable to get to the office, you can lose critical hours or days of business continuity and productivity.

With a secure digital workspace, people can access all their apps and data using their home PC, laptop, or even their smartphone—with the same familiar experience they would have at the office. The ability to continue work without losing time, data, or collaborative contact with their teams not only keeps the business moving forward; it can also help people feel empowered and confident as they bounce back from the disruption.

Increase business agility

Traditional processes for onboarding employees and opening branch offices are a model of inefficiency. Admins create images of a standard, approved desktop with the appropriate apps, download the image onto the desktop or laptop, and then either wait for the employee to physically pick it up at the office, or else pack and ship it to them. Future app updates follow a similar process. This time-consuming, labor-intensive approach delays the impact of key hires and strategic initiatives.

With a secure digital workspace, employees can buy any type of device they want and simply log into the company network to be automatically provisioned with corporate-approved apps pre-configured with the right security controls. Able to expand and grow more efficiently and securely, the company can realize the improved business agility promised the cloud.

Ensure business continuity

Responding to a disaster (natural, IT, cyber, civic) can be a slow and messy process. If your strategy depends on procuring and configuring more PCs, and then distributing them to users unable to get to the office, you can lose critical hours or days of business continuity and productivity.

With a secure digital workspace, people can access all their apps and data using their home PC, laptop, or even their smartphone—with the same familiar experience they would have at the office. The ability to continue work without losing time, data, or collaborative contact with their teams not only keeps the business moving forward; it can also help people feel empowered and confident as they bounce back from the disruption.

Business continuity
and
disaster recovery

top the list of most important technology projects
IT departments are currently working on[6].

CITRIX®

As modern hybrid and multi-cloud IT environments become more complex, a secure digital workspace makes it possible to deliver a better experience for workers while strengthening security and simplifying IT—so the business can realize greater value at each stage of their cloud journey.

If you're interested in exploring the potential benefits of a secure digital workspace for your organization, we encourage you to explore Citrix Workspace at:

citrix.com/products/citrix-workspace/

Source:
1. "IDG Cloud Insights 2018" report.
2. How do Organizations Plan to Assure Application Delivery in a Multi-Cloud World? IDC Infobrief, October 2017.
3. "The Need for a New IT Security Architecture," Ponemon Institute, sponsored by Citrix, 2017 .
4. "Remote Workforce NPS: The Most Important Metric You're Missing," Business 2 Community, March 2017.
5. "Number of network connected devices per person around the world from 2003 to 2020," Statista.com.
6. CIO Tech Poll: Tech Priorities 2018, IDG.