Preparing for the Workspace of the Future

A guide to unifying, simplifying, and securing cloud services

Table of Contents

Working Toward Tomorrow's Workflows

Future work environments will no longer tether employees to their desks, offices, or even devices. Rather, they will unify all cloud-based and physical resources that people need to do their jobs—and do so in a more secure and contextual manner than anything available today.

In the past, you began your day on a physical device that was dedicated just to you. Your data, applications, and login were all contained in a single space. But now, the center of work is shifting away from the device to the cloud. Indeed, many of your frequently used applications (and even productivity tools) are now cloud-based software as a service (SaaS) apps. But as SaaS application offerings help to quickly address these new needs, you suddenly find yourself with multiple logins, data sources, and security risks that are growing at a dangerously rapid rate. As a result, enterprise IT is even more concerned over reduced control, insight, and governance over the SaaS apps that employees are using; the state of sensitive data in those apps; and the way to integrate those SaaS apps into the fabric of the company.

As workers continue to consume more cloud services, enterprise IT is evolving toward a **secure digital workspace platform**. This will give IT administrators a streamlined insight into and governance over how SaaS, web, and even local apps are secured and presented to users—providing a new way for employees to begin their day, securely accessing those apps in a more personalized manner.

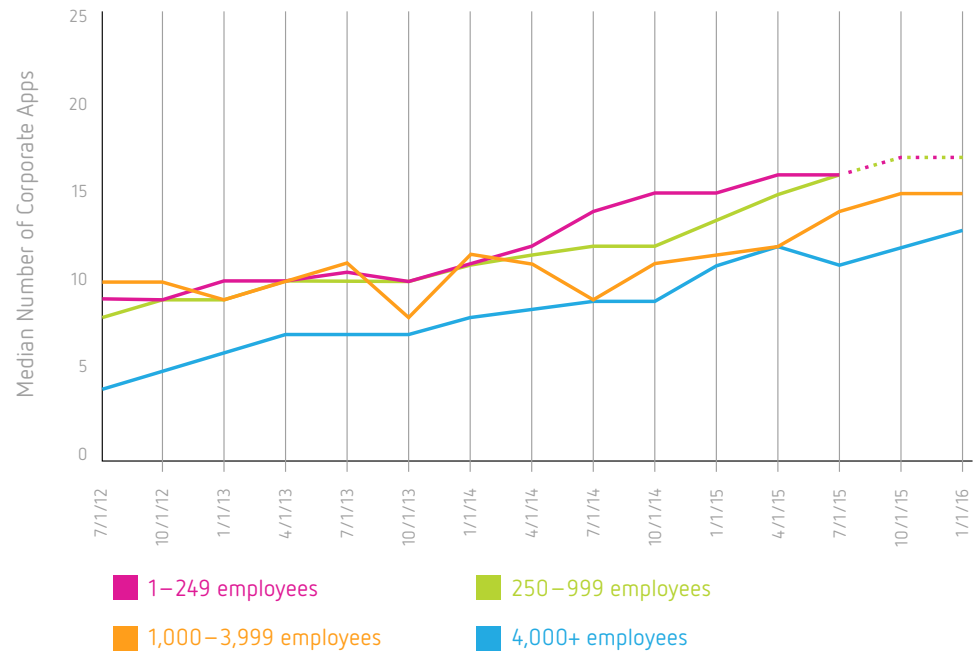
The Evolution of the Workspace

To really understand the problems organizations face when embracing this new work environment, we have to understand how we've gotten to this point.

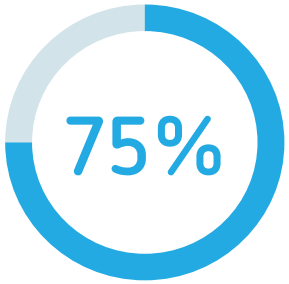
Workers traditionally started their days at their desks, in front of their desktops. Logging into their computers gave them access to everything they needed to complete their tasks: connecting them to programs, the company server, important documents, and more. Network security was often limited to the business' premises and proprietary network, and it could easily be managed by IT teams.

But as internet services expanded, browser-based SaaS apps have proliferated. Businesses have become more confident in vendors' abilities to provide secure best-of-breed solutions for their organizations' needs—likely going to one company for payroll, another for project management, and another still for sales. As enterprises more readily adopt this strategy, they end up with an increasing number of disparate cloud service providers.

Median Off-the-Shelf Cloud Apps, by Company Size Over Time[1]



The growth in cloud service adoption is changing how employees access their work, swapping desktops for internet browsers.

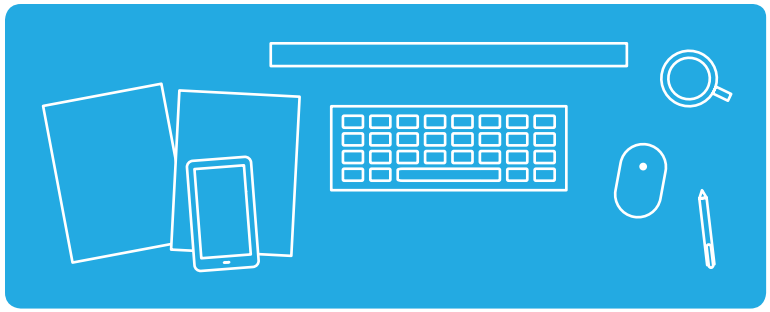


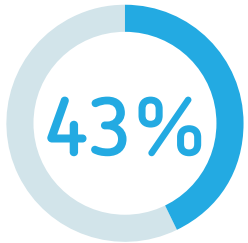
of enterprise workloads now run in the cloud.[2]

SaaS applications have created 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:

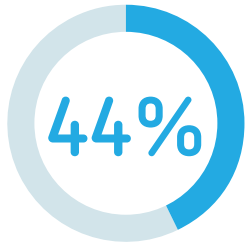
- Be productive from anywhere with an internet connection.
- Use their favorite devices, whether desktop computer, laptop, tablet, or smartphone.
- Pull up key documents in important meetings, no matter where they're held.

Rising Mobile Access Demand in the Workplace[3]





of surveyed professionals see the use of mobile devices as very critical for work.



check or use a mobile device for work more than 20 times per day.

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

Current Workspace Challenges

While incredibly beneficial, the way we currently work also brings a number of unintended consequences. With so many sanctioned (and unsanctioned) SaaS applications, network complexity and security risks are unavoidable.

Multiple logins, fragmented access:
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.

Non-contextual 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.

No integrated workflows:
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—but without a process and workflow to keep the two in sync.

Inconsistent 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.

Current Workspace Challenges (cont'd)

Different end-user experiences:
Cloud applications are often optimized for different browsers, devices, or operating systems, leaving employees with disparate 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.

No master 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.

No holistic insight and analytics:
Disconnected (or nonexistent) 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.

Broken IT 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.

One solution to this complexity and risk is for IT management to halt the adoption of SaaS applications. But this knee-jerk response from IT would put them at odds with lines of business that demand to use these apps—driving users further into using "shadow IT," where administrators would have even less insight into the SaaS apps being used.

Examples: The Problem With...

Adoption on non-sanctioned applications:
Employees adopt a popular instant messaging application that they use broadly. Although sanctioned by IT, it has no SSO or governance oversight. This opens up security holes (a) when employees connect other "plugins" to the app, and (b) when employees leave the company, taking their accounts (and all sensitive posted data) with them.

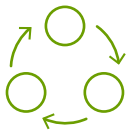
Lack of contextual access:
Employees use a popular app delivered by IT. But due to a hacking intrusion, an employee's device has been compromised. Without contextual security, the system fails to notice that access from one employee-owned device corresponds to a secure on-premises network, while the other device is concurrently accessing the app from an off-premises network thousands of miles away.

The lost productivity, lack of oversight, and security risks ultimately threaten your company's bottom line. But there is a way to simplify management while still utilizing the best-of-breed SaaS applications your organization has come to rely on.

The Solution:
A Secure Digital Workspace

Seemingly overwhelming, these challenges can create a culture that forces IT management to say no. Rather than locking down users, apps, and networks, an alternative approach is to fully embrace this shift to a cloud-centric, SaaS-centric world. A secure digital workspace environment solves these issues, while helping facilitate all the benefits of adopting external cloud and SaaS applications.

Single sign-on:
SSO lets users log in once to access all of their cloud applications. It also permits IT to grant and revoke global employee access during onboarding/termination.



Integrated workflows:
Provide logical integration between applications, as well as a stateful application environment for employees to work.

Consistent user experience:
Ensure that, no matter what application is paired with what device, the experience is consistent, the performance is near-native, and the application functionality is automatically adapted to device features.

Contextual security controls:
An adaptive approach to creating a "software-defined perimeter," security and rights are applied in a contextual manner, based on devices, networks, locations, and user behavior.

Contextual access:
With more granular insight into devices, networks, application needs, and security stance, IT can grant user access (or partial access) to approved devices and locations. That way, IT can be confident about maintaining a security posture, while providing users with the best possible access to their workspace.

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 to provide actionable insights for the organization.

Governance in IT's hands:
With a single control panel across all cloud applications, IT can easily manage data across your organization.

The new secure digital workspace will play a vital role in the future, enabling businesses to realize the full benefits of the cloud while avoiding the complexity and security challenges that have come with its widespread and uncontrolled adoption.

"Today's workers seek to make the same kinds of choices they do as consumers. [...] IT leaders can give them that choice by employing the digital workplace: a business strategy to promote employee agility and engagement through a more consumer-oriented work environment."
— Gartner [4]

Start Your Cloud Journey Where It Suits You Best

Citrix's secure digital workspace approach provides organizations and their employees with reliable app and data access, as well as a seamless experience across all their devices. It also arms IT with a single control plane to configure, monitor, and govern it all. This reduces complexity and risk, so IT and organizations can fully embrace cloud-based services with trust.

Major Benefits

Enabling an adaptive experience:
A unified cloud platform enables a workspace experience for the enterprise user that optimizes their day-to-day productivity and enriches the experience of both knowledge workers and task workers. In addition to delivering rich productivity apps to enterprise desktops, laptops, and mobile devices, it enhances the user experience with tightly integrated apps and enables collaboration with secure document management and IoT-enabled workflows.

Collecting, analyzing, and applying intelligent context using security and behavior analytics:
By contextually delivering apps and data based on user and entity behavior, end-point, and network environments—as well as by providing always-on proactive insights from data in motion/at rest/in use—the platform ensures optimal application performance and mitigates the risk of threats to infrastructure, data, and apps.

Unifying hybrid cloud service delivery:
Whether provisioned as an IT service from the enterprise data center, one or more third-party clouds, SaaS providers, or a mix of on-premises and public cloud services, the platform provides secure access to data and apps. It delivers high security to any end-point, whether on a corporate-owned or unmanaged employee device.

Unify Cloud Services with Citrix

As mobility continues to evolve the way we work, companies need to address all the associated complexities and risks head-on. Securely unifying your cloud services will empower your employees to work from anywhere, while giving IT additional control, governance, and peace of mind.

The Citrix and Intel partnership continues to ensure your cloud solution is optimized to deliver powerful, efficient cloud solutions that provide better virtualization, security, and analytics. No matter where you are in your cloud journey—on premises, hybrid cloud, or public cloud—Citrix and Intel partner to meet you there. Leading cloud provider data centers run on Intel® architecture.

Move your business to the workspace of the future, today.
Visit citrix.com/cloud.

CITRIX®

intel XEON inside

Sources:

1. "Business @ Work," 2016, Okta
2. "State of the Cloud Report," 2017, RightScale
3. "Released: 2016 Mobile Productivity Report," 2016, Wrike
4. "Gartner: Predicts 2017: Boosting Business Results Through Personal Choice in the Digital Workplace," November 14, 2016, Paul Miller, Nikos Drakos, Carol Rozwell, Matthew W. Cain, Jeffrey Mann, Jim Murphy, Mike Gotta, Adam Preset, Gavin Tay