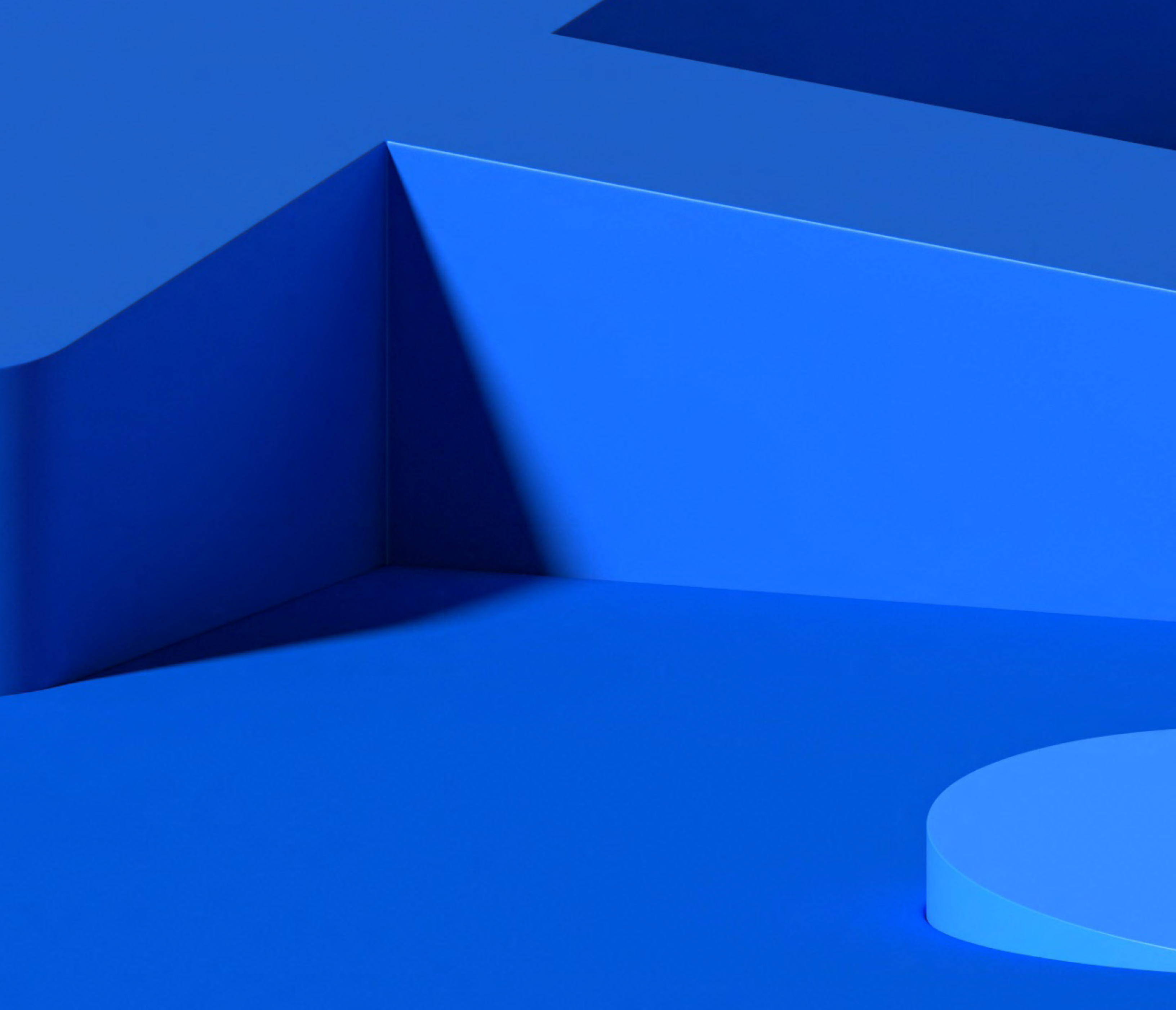
White Paper

On-Premises to Cloud

A Workspace Service Journey

Enable secure, flexible work for every type of worker with Citrix Workspace Services.



Contents

Executive Summary

The global pandemic has necessitated a new mode of remote work, and post-COVID forecasts are pointing to more flexible workplace environments and policies. A Citrix and YouGov study reveals that 66% of respondents believe people will never return to the office full time.[1]

IT teams continue to prove their mettle, enabling flexible work, while a traditional, on-premises deployment for virtual apps and desktops reaches its physical capacity limit. A LogicMonitor Cloud 2025 Survey reveals that 87% of enterprises will accelerate their cloud migration in the near future.[2]

Citrix Workspace, with expanded intelligent features and capabilities, helps your IT teams deliver optimal employee experiences, for every type of worker—whether they're at the office, at home, or back on the road. Give them secure access to apps, files and data — everything workers need for peak productivity, where and when they need it— all leveraged from within your existing infrastructure.

In this paper, we'll guide you through the landscape of Workspace, past, present and future. You'll get practical, incremental steps to scale your Workspace deployment into an ever-ready state to seamlessly deliver the future of work.

At every point in your journey, count on 3 key business values:

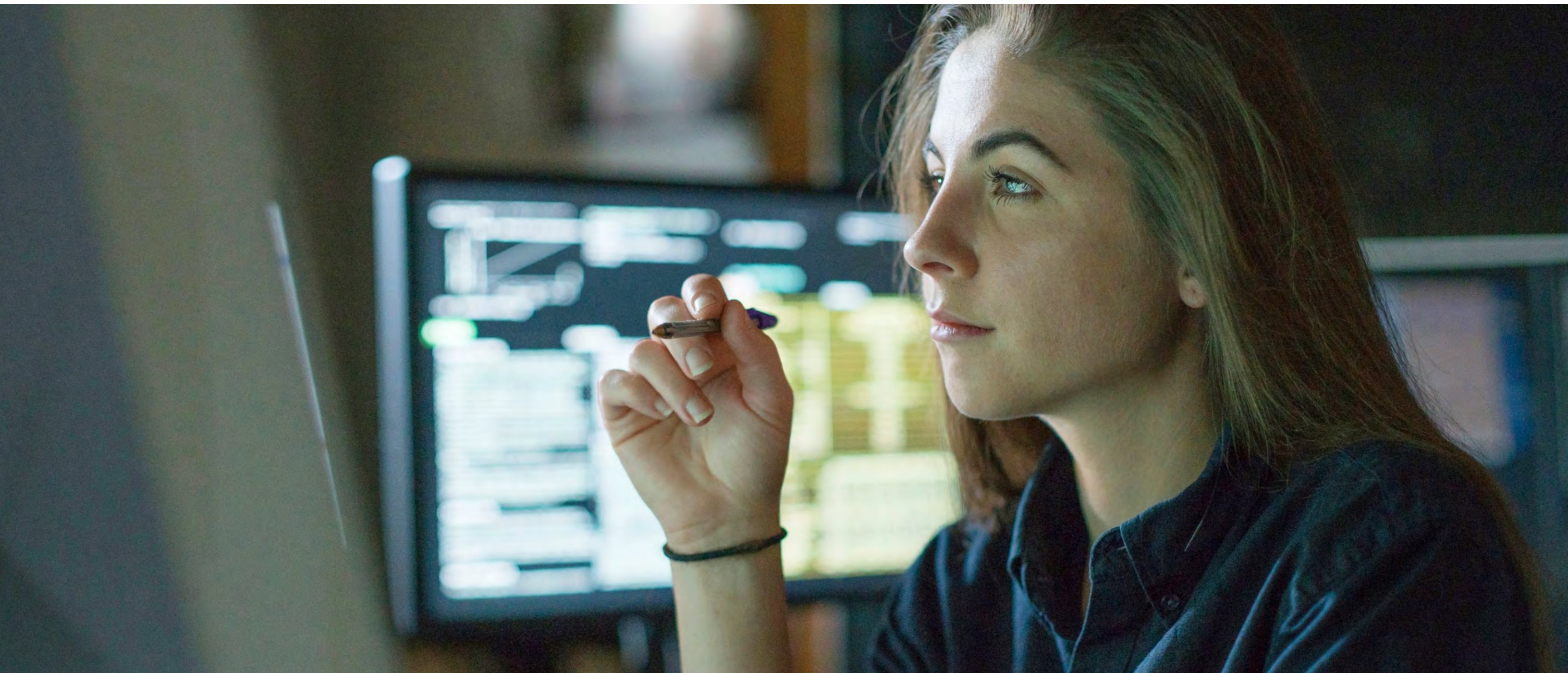
- ✓ Faster time to value: Deploy workloads up to 4 times faster from any cloud, on-premises data center, or hybrid model.[3] Simplify on-boarding for mergers and acquisitions, new employees, contractors, and a myriad of business-critical use cases.
- ✓ Deployment flexibility: Adopt public clouds at your own pace, support new workloads, encourage business continuity expansion, or accelerate into the cloud as needed. Transition on-premises deployments to hybrid/cloud resource locations in a time frame that aligns with business needs.
- ✓ Simplified management, security and business continuity: integrated cloud services simplify management of on-premises and cloud-hosted resources. Reduce public cloud costs by up to 80%, streamline business continuity and disaster recovery planning, and secure sensitive intellectual property.[3]

Sources:

[1] https://www.citrix.com/fieldwork/flexible-work/tomorrows-office.html

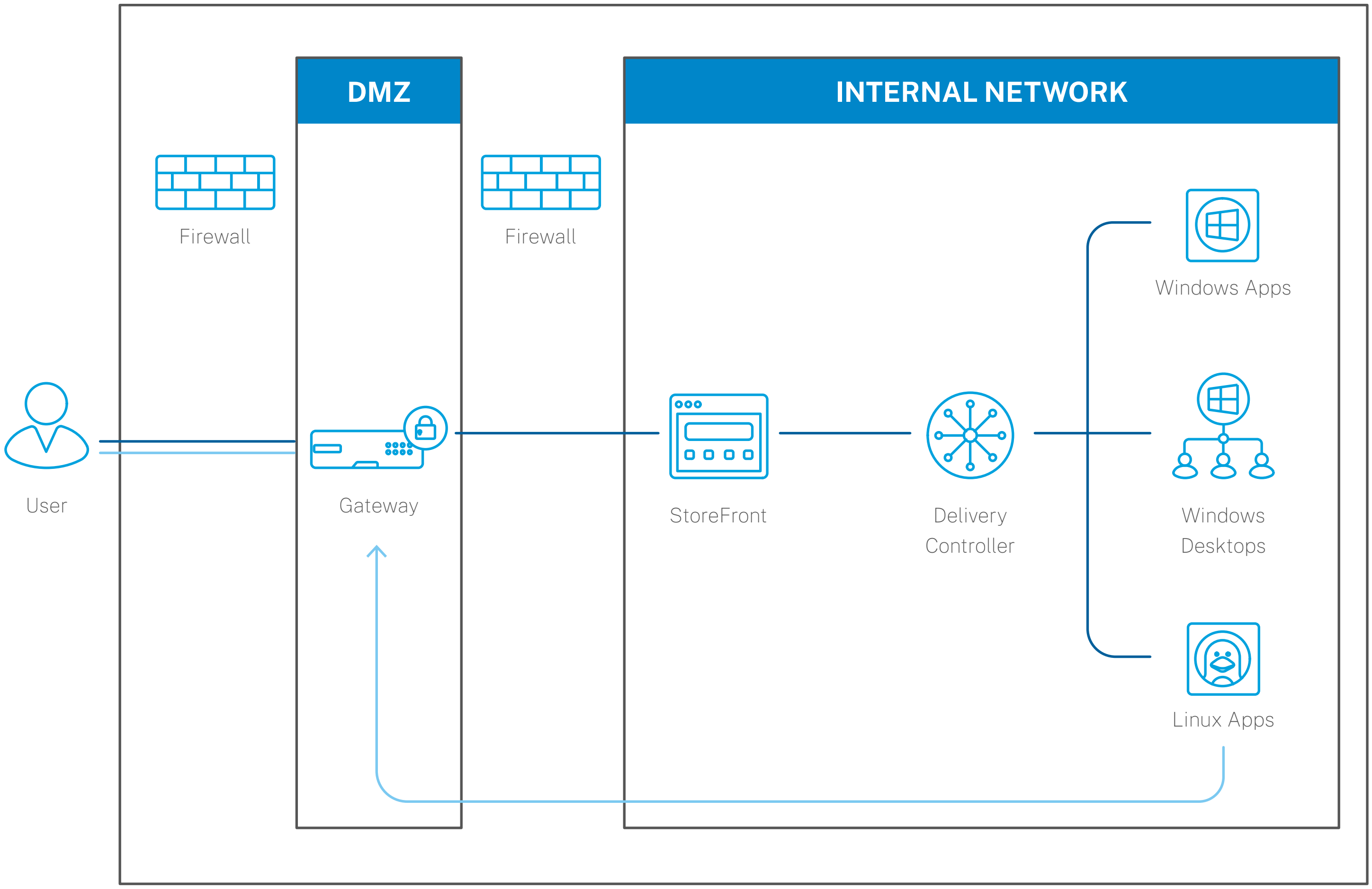
[2] https://www.logicmonitor.com/resource/cloud-2025

[3] Citrix, Business Value of Citrix Virtual Apps and Desktops service White Paper



Past Tense: Traditional On-Premises Deployments

While a major shift is underway in how businesses enable access to a growing array of apps and content, it's useful to travel back in time to recall a traditional PC environment. In those days, IT admins centrally managed desktop and app delivery. As virtualized apps and desktops became standard, they were deployed in an on-premises data center. IT was tasked with wrangling the core delivery components and the associated infrastructure hosting the applications and desktops.



On-Premises (IT Managed)

The characteristics of an on-premises workspace may still ballast many businesses in an increasingly cloud-based world. Here's how that model looks:

- ✓ Workers operated all work functions from a single device
- ✓ All content was a combination of local and network storage
- ✓ Work apps were largely Windows-based
- ✓ All users were mandated to be physically present

The lift for IT was daunting. Frequent updates, device upgrades, and patching meant many long nights and weekends for teams managing the on-premises gauntlet. While the advantage was control over access, virtual machines, applications, desktops, and security, the churn took its toll on efficiencies and costs.

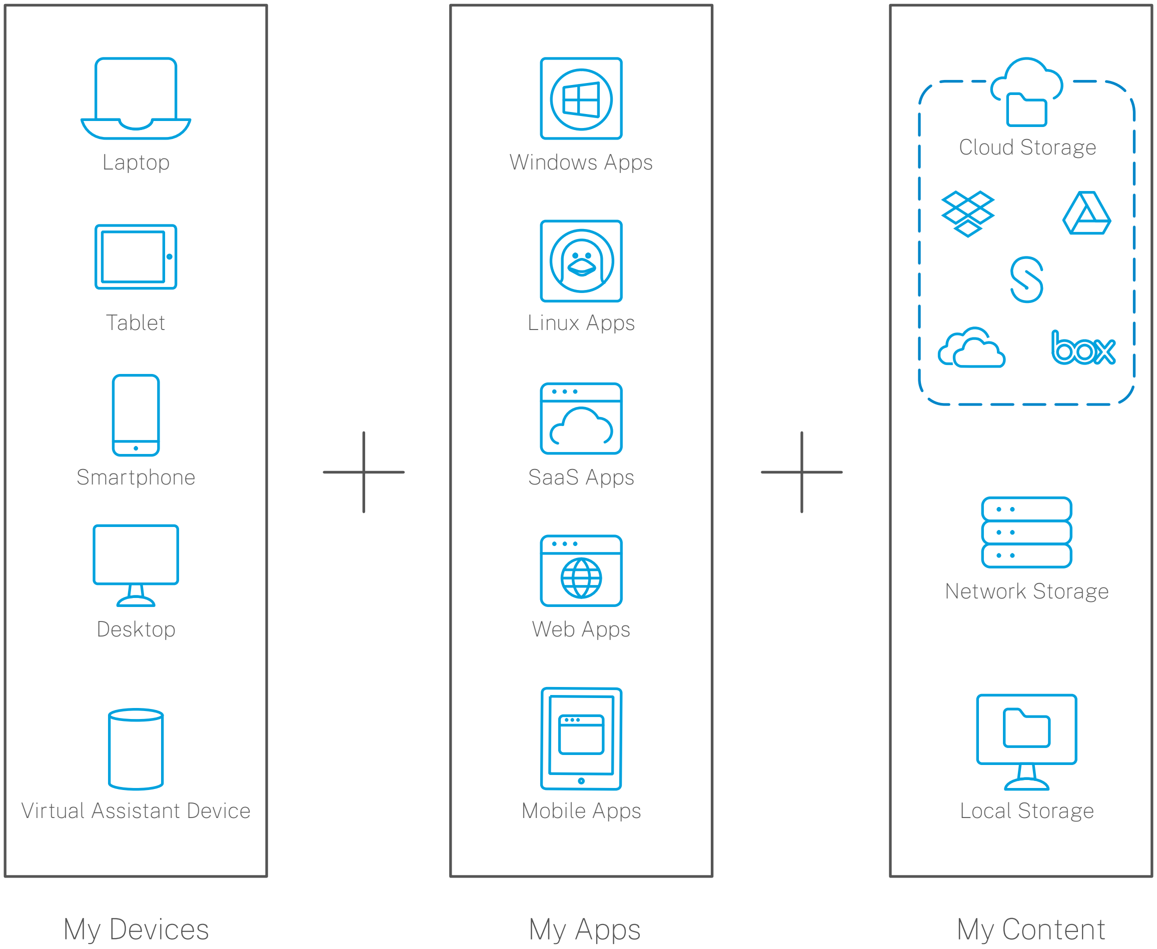
User experience was often dictated by the single device available to each worker. As mobile devices emerged, workers were urged to adapt to a workspace unique to mobile. As demand required multiple devices per employee, workspaces further fragmented, with each device carrying its own adventure for the weary worker.

The need to to unify employee experience and create a manageable model for IT teams drove the creation of Citrix Workspace Services. By leveraging cloud-based architecture, organizations are able to seemlessly connect resources and deliver **more immediate value, flexibility, agility** as well as **simplified management and security**.

Present Tense: A Fragmented State

For organizations in nearly every sector, 2020 required an adaption of the traditional on-premises model to one that enables primarily remote work, leading to a strain on infrastructure flexibility and security. Long-term, strategic plans to migrate legacy workspaces to the cloud suddenly became sprints to ensure business continuity, data security, and worker productivity.

Today's workspace environment has evolved into an intricate collection of devices and applications for each user, complicating access and security across the organization.



VPN, once the entry point for an organization's road warriors, has also reached its limit with the remote—and fast-becoming flexible—workforce, creating exponential endpoint expansion. Security risks lead to the endless addition of point products like SSL VPN, single sign-on, and endpoint management, to stay on top of new security cases.

With remote and contract workers having to rely on their own devices, the "bring your own device" (BYOD) surge only adds to the complexity. A contextual security framework, with continuous authentication and verification, is the clear way to grant access to the growing number of web and mobile apps workers need to get work done. A Zero Trust security model provides partial access to your network, as needed, while monitoring aberrant user behavior.

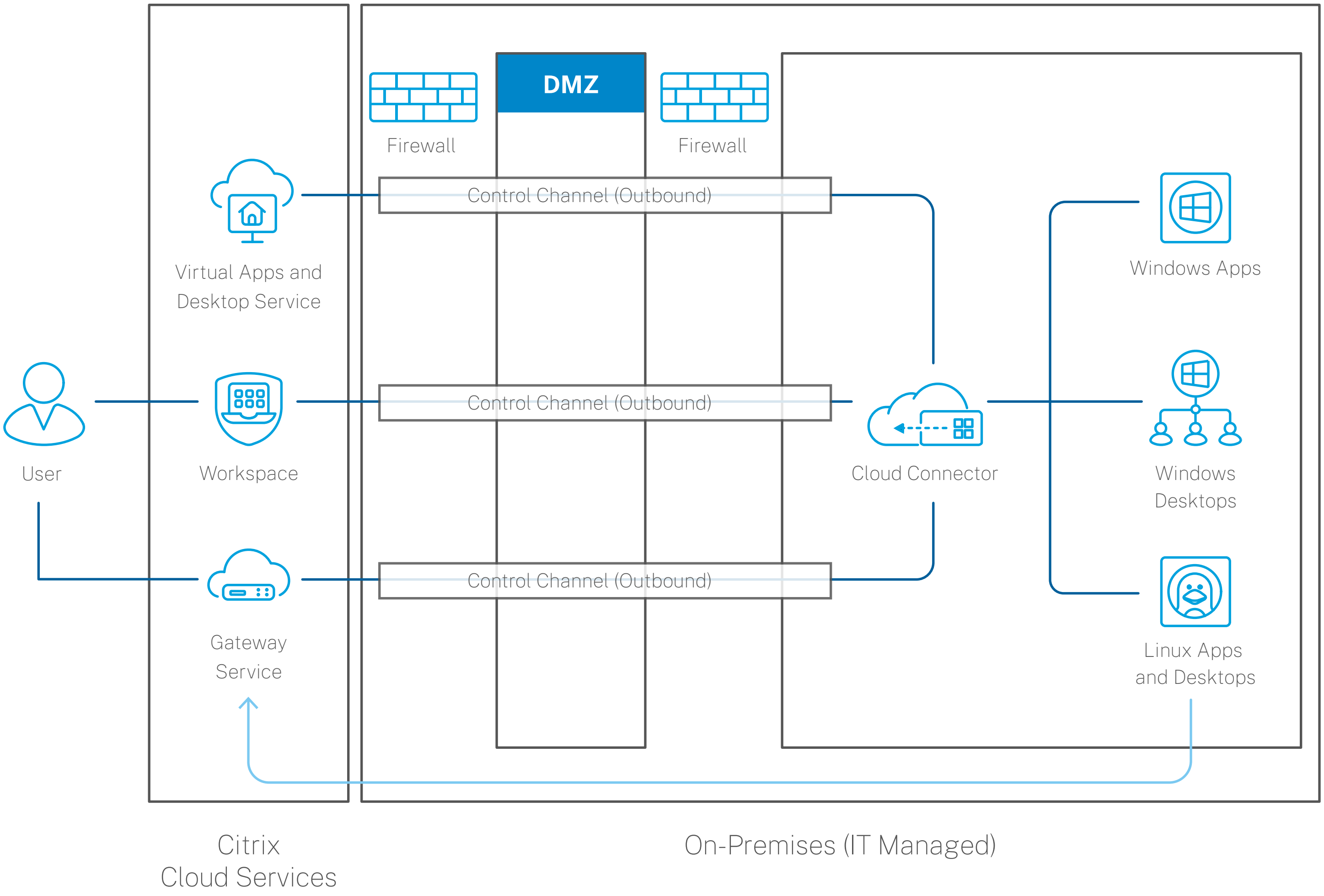
The challenge for technology providers and IT teams now is to unify and simplify environments and experiences. The emerging workforce is accustomed to simple, powerful digital engagements, and from a manageability perspective, IT teams can stand to be spread less thin. It all comes together with Citrix Workspace Services.

Future State: Becoming Cloud Friendly

Ideal Workspaces:

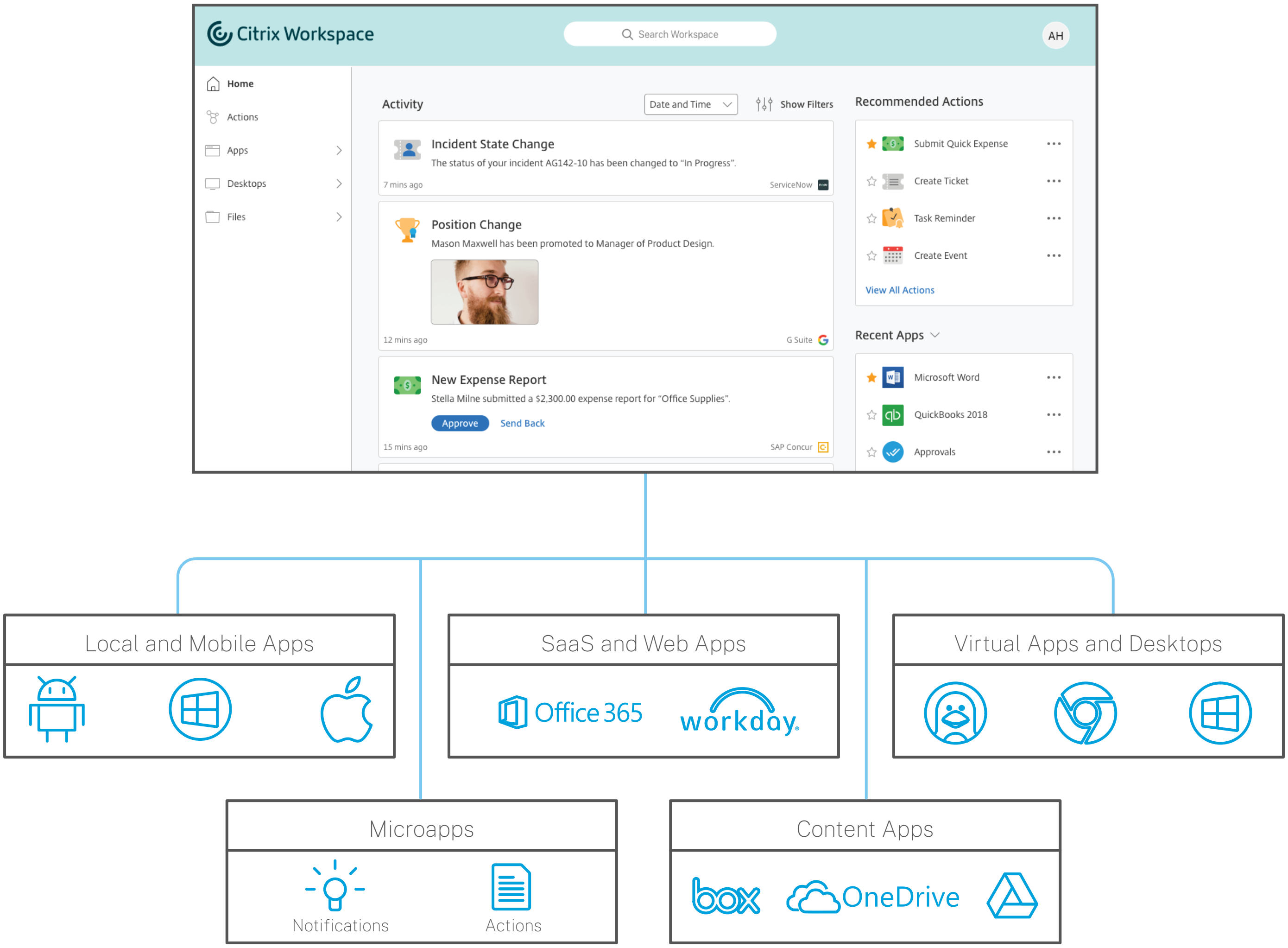
- ✓ Unified and simplified technology
- ✓ Reliable, consistent, and optimal user experience across devices
- ✓ Enhanced, contextually aware security
- ✓ Maximized productivity for every type of worker

With the emergence of cloud-based content and apps, migrating from a strictly on-premises model is a top priority in most organizations. Moving the management layer of your Citrix Virtual Apps and Desktops deployment to Citrix cloud service reduces the complexity of installation, setup, management upgrades, and integrations.



With Citrix Virtual Apps and Desktops Services, you can have on-premises or cloud-hosted resource locations, giving you secure management of your legacy apps, files, and data, without the complex networking of infrastructure configuration. Now your IT teams can focus on the resources that provide the most value to your users.

From a user perspective, they get a unified, simplified, and consistent experience across devices. Citrix Workspace delivers local SaaS, web, mobile, browser, and content apps and files—all within a simplified, prioritized UI, personalized for each worker. And the optimal, and constantly optimized, experience is the same whether workers are at home, on the go, or in the office.



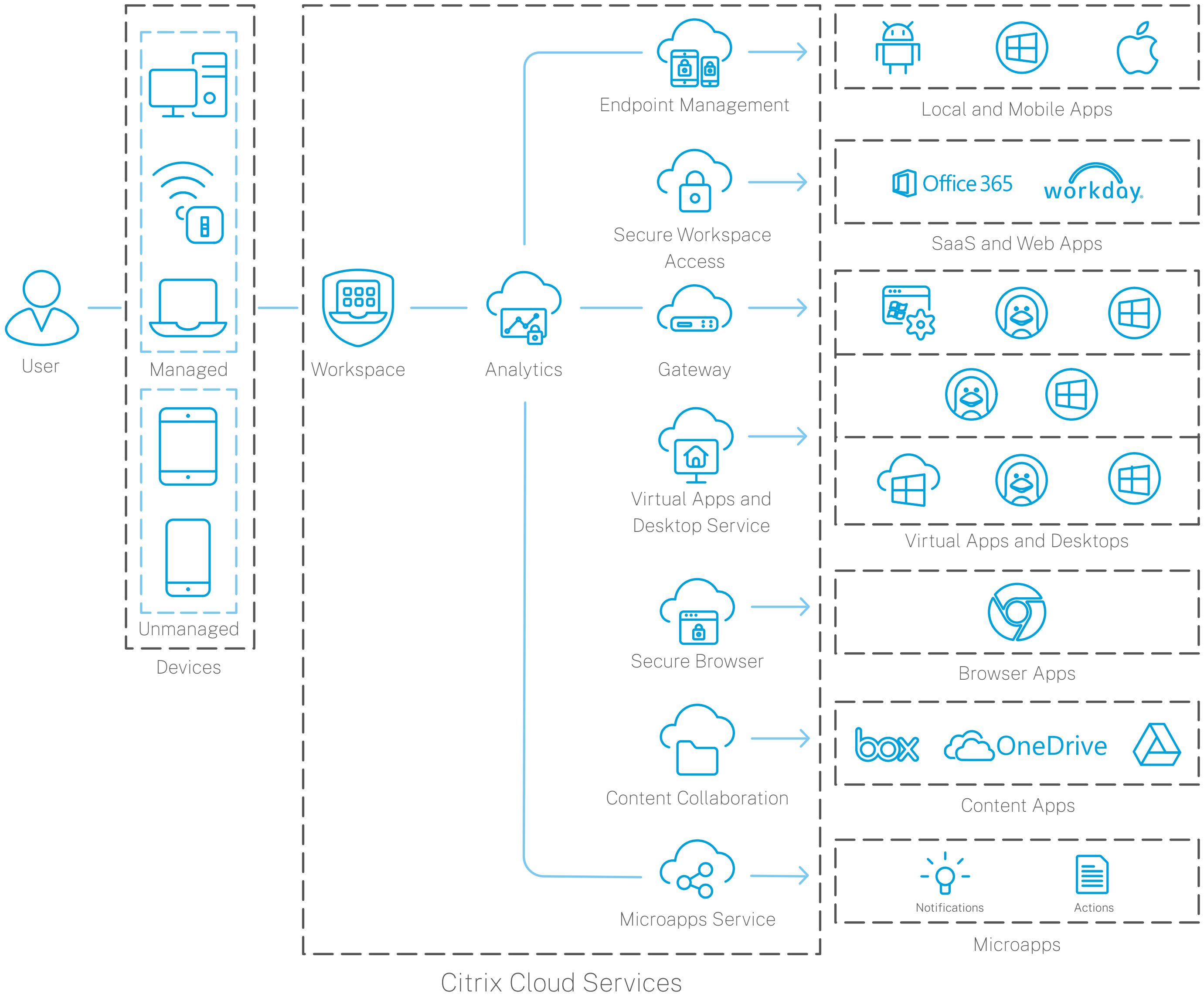
Incident State Change
The status of your incident AG142-10 has been changed to "In Progress".
7 mins ago · ServiceNow

Position Change
Mason Maxwell has been promoted to Manager of Product Design.
12 mins ago · G Suite

New Expense Report
Stella Milne submitted a $2,300.00 expense report for "Office Supplies".
15 mins ago · SAP Concur

With the future of work ahead, there is still another level to achieve—a unified workspace platform that simplifies environments and offers the fastest possible path to ROI and realized business value. Securing and enabling a growing flexible workforce and future-proofing your organization is of the essence: enter Citrix Workspace.

Optimizing employee experience, including creating a secure, manageable environment that dynamically scales for the demands of the future of work, begins by taking these steps to take full advantage of all that Workspace can do for your IT teams, workers, and organization.



Step 1: Utilize Citrix Workspace Experience With Virtual Apps and Desktops + Analytics

Deliver a unified, compelling user experience by aggregating on-premises and cloud-hosted apps, plus desktops into a consolidated identity with Citrix Workspace.

IT Benefits:

- ✓ Cloud service, providing remote access to virtual desktops, apps, and browsers
- ✓ Integration of identity provider
- ✓ Site aggregation, integrating existing CVAD deployments
- ✓ Secure and optimized connectivity to backend resources
- ✓ User and device behavior monitoring and risk analysis
- ✓ Proactive performance monitoring and the ability to isolate root causes and address prior to experience degradation
- ✓ Seamless evergreen auto-update and centralized management
- ✓ Efficient user onboarding
- ✓ Hybrid cloud flexibility
- ✓ Autoscaling cloud resources to control costs
- ✓ Reduced management overhead
- ✓ Eliminates the need for an on-premises delivery controller, license server, and SQL server

Added Features:

- ✓ Providing users with a unified digital workspace experience with the choice to use any device and any network to access any of their enterprise apps, desktops, and data in a virtualized environment
- ✓ Consistent experience across any device
- ✓ Detect and prevent insider threats with user behavior analytics
- ✓ Optimize user experience with performance analytics

Business Value:

- ✓ Reduce overhead and control costs
- ✓ Increase time-to-value of end users by faster onboarding
- ✓ Improve overall experience, helping improve the technology employee experience
- ✓ Moving to Citrix Virtualized Apps and Desktops service—speeds up adoption of new features, leading to increased revenue and productivity, and allowing the business to respond to strategic needs faster

Stop security breaches before they happen:

- ✓ 212 days: average time to identify a data breach[1]
- ✓ 20% — breaches caused by compromised credentials[1]

Source: [1] https://www.ibm.com/security/data-breach

> **“Now is not the time to pull back on workforce development efforts, but instead to double down on commitments to building a resilient workforce that can adapt in the face of constant change.”**
>
> – Deloitte, *Returning to Work in the Future of Work*

Step 2: Provide Zero-Trust Access and Integrate SSO to Apps

With a consolidated identity to your on-premises applications, securing your Web and SaaS apps is your next step.

IT Benefits:

- ✓ Cloud native VPN-less access to SaaS and Web apps with enhanced security
- ✓ Enforce enhanced security controls for accessing data within SaaS and Web applications
- ✓ Protects user from accessing malicious and non-approved websites
- ✓ Integrated isolated browser provides flexibility to use BYO device to access sanctioned apps securely
- ✓ Protect user and corporate data from being stolen by keyloggers and screen capturing malware

Added Features:

- ✓ Web Isolation and Secure browsing
- ✓ SSO with 2FA for SaaS/Web/Virtual apps
- ✓ Enhanced security policies around SaaS/Web Apps such as restricting clipboard access, printing, downloads, and displaying a watermark
- ✓ Centralized and contextual secure access policies across all apps

Business Value:

- ✓ Savings in support tickets thanks to SSO: $5,401,260[1]
- ✓ Productivity improvements per app per month due to faster deployment of apps: valued between $900,000-$3,250,000[1]

Source: [1]https://www.citrix.com/content/dam/citrix/en_us/documents/other/the-business-benefits-of-enabling-the-modern-workspace.pdf

Step 3: Unify, Secure, and Digitize User Content and Document Workflows

Jump-start productivity by enabling workers to access data from any source, on any device securely, while automating document workflows to solicit feedback and expedite approvals with integrated electronic signature. All while eliminating consumer file-saving service threats and protecting data with a robust feature set.

Benefits:

- ✓ Deliver a consumer-like content experience across all devices without needing to migrate data to the cloud
- ✓ Unify disparate repositories
- ✓ Eliminate threats posed by employee file-sharing and provide a comprehensive set of data protection features

Added Features:

- ✓ Ability to search across apps and files
- ✓ Mobile app integration
- ✓ SSO across mobile apps
- ✓ Apps and files integration
- ✓ Content workflows

Business Value:

- ✓ Digitize workflows, increasing efficiency by +20%
- ✓ Global average cost of a data breach — $4.24 million[1]

Sources: [1] https://www.ibm.com/security/data-breach

Step 4: Streamline Common Workflows with Microapps

Create action-oriented workflows for busy users with low-code micropps from legacy, on-premises, and SaaS apps. Admins configure, build, and modernize custom microapps directly from the Citrix Cloud console, focusing and facilitating tasks into a seamless personalized flow, eliminating time lost to context switching.

Intelligent Microapps

Applications are powerful but can be cumbersome for routine or simple tasks. Leveraging publicly available APIs within SaaS, Web, legacy, and homegrown applications, microapps allow users to view information and perform actions without requiring a full launch of the application. A personalized, simplified Workspace feed provides users with a central location to perform those actions, doing away with counter-productive context switching.

Benefits:

- ✓ Modernize applications by delivering key actions and notifications in a simple, personalized UI
- ✓ Empower IT to securely deliver the premier digital workspace experience, with built-in low-code tooling as well as easy-to-use integrations for apps and integrations with identity providers. Provision, manage, and monitor the entire workspace infrastructure through a unified management console
- ✓ Reduce training and education of new apps and features by utilizing microapps
- ✓ Design workflows for all apps—Web, SaaS, and on-premises

Added Features:

- ✓ Activity feed, including actions and notifications to SaaS/on-premises apps
- ✓ MS Teams Integration
- ✓ Microapp builder

Business Value:

- ✓ Employees can save up to 4 hours/week[1]
- ✓ 18% productivity improvement for fully engaged employees[2]
- ✓ 2.5x revenue per employees versus competitors with low engagement[3]
- ✓ Generate 21% higher profitability per employee than lower quartile companies[4]
- ✓ Helpdesk costs—$50/ticket with average employee making 6 calls per year[2]

Sources: [1] McKinsey Insights

[2] https://www.citrix.com/content/dam/citrix/en_us/documents/other/the-business-benefits-of-enabling-the-modern-workspace.pdf

[3] Hay Group

[4] Gallup

Step 5: Consolidate Management and Protect Access on Devices

Manage, secure, and inventory a broad range of devices from a single management console.

Benefits:

- Use a common set of device policies to manage supported devices.
- Protect business information with strict security for identity, corporate-owned and BYO devices, apps, data, and network. Specify user identities available to authenticate the devices. Configure how to keep enterprise and personal data separate on devices.
- Deliver any app to end users, regardless of device or operating system. Protect your information at the app level and ensure enterprise-grade mobile application management.
- Use provisioning and configuration controls to set up devices. Those controls include device enrollment, policy application, and access privileges.
- Use security and compliance controls to create a customized security baseline with actionable triggers. For example, lock, wipe, or notify a device in violation of defined compliance standards.
- Use OS update controls to prevent or enforce operating system updates. This feature is critical for data loss prevention against targeted operating system vulnerabilities.

Added Features:

- Support for multiple use cases within a single deployment (enhanced enrollment profiles)
- Full support for Android enterprise
- Single policy push to specific devices for user reconfiguration
- Additional policy support for macOS
- Device grouping for Windows 10 devices
- Management and delivery of Office 365 apps
- Full support for iOS user enrollment
- Enhanced reporting for device compliancy

Business Value:

- Enhanced visibility for device compliance (City of Oulu)
- Enhanced contextual security: providing MDM and MAM policies that can trigger automated actions
- Low-touch, no-touch deployments that enable over-the-air (OTA) out-of-box user experiences
- Reduce reliance on the Help Desk team
- Avoid major security incidents and data breaches[1]

Source: [1] https://www.citrix.com/content/dam/citrix/en_us/documents/other/the-business-benefits-of-enabling-the-modern-workspace.pdf

Conclusion

In the space of a year, it became clear that change is the one thing we can count on. As more content and applications shift to the cloud, IT teams are carefully considering hybrid or full-cloud environments to reduce the resource expenditure of perpetually licensed software, updates and deployments. Post-Covid, workers will expect greater flexibility around working environments and tools, all of which require contextual, secure access and optimal application performance. The clear evolution is Citrix Workspace: meet these challenges with a flexible, intelligent, unified Workspace experience, on any device for every kind of worker.

Unify and simplify your technology environment with a full-featured platform that provides the **fastest path to value,** enhanced **flexibility and agility,** and **simplified management and security.**

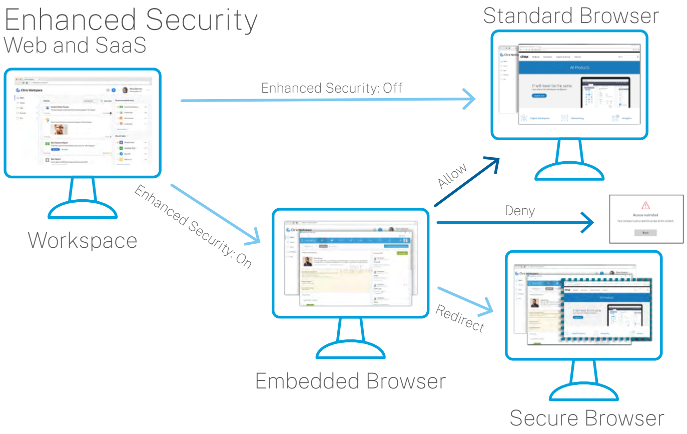
Learn more about Citrix Workspace

Connect with a Citrix specialist

Index

1. Enhanced Security

a. Enable end users to access grey-listed sites, including personal email, through advanced embedded and secure browsing



2. Encompass local apps, mobile apps

a. On many devices we have personal apps and we have work apps.

b. This isn't limited to phones on iOS and Android; Windows also has this.

c. Personal apps and work apps
   i. How do we protect the work apps?

d. With app containers, we can separate our work apps from personal apps.

e. Once the app is in a container, we can control app-to-app interactions.
   i. The container also carves out a secure set of resources that are only accessible from the apps within the container.
   ii. The work apps and associated containers are configured with centralized policies that can require a passcode to use the app. Restrict the app from running on jailbroken devices, as well as define if and how the app can communicate with backend resources, via a micro VPN.

f. The challenge with mobile users is that they are not always located within the confines of the data center.

g. External access to internal resources is protected by a firewall. Somehow, we have to allow these devices through the data center's firewall while also protecting public.
   i. Traditionally, we would provide a full VPN into our data center. However, there are a couple problems with this approach.
   ii. Problem 1: A full VPN is device-level. Meaning that every app and component on the device has access to our internal resources.
   iii. Problem 2: A full VPN gives the user keys to the entire castle. That means this one connection allows the device, and every app on that device, to have access to every resource within our internal network.

h. An alternative approach is to replace the full VPN with a micro VPN.
   i. App-specific. Only those apps granted micro VPN access can establish a tunnel.
   1. Only gets established when the app is running—prevents battery drain.
   ii. Resource-specific. This means that a certain endpoint app can only access a certain internal resource.

3. Content Collaboration

a. There are challenges with how we handle content in an environment where users have multiple devices; some are trusted and some are untrusted, some are physical and some are virtual, some are persistent and some are nonpersistent.
   i. From all of these devices, users need access to their content, which could be any cloud provider, local storage, or network storage.
      1. How do users configure their endpoints to access this content from all types of endpoints? Is the experience the same or different?
      2. Finally, what security is incorporated into all of these content repositories and how are they applied on different endpoints? Can we allow third parties access? What can they do (edit or view)? Can we remotely wipe data from devices? Can we secure the data?
      3. How do we make typical activities easier for users?

4. Security Analytics

a. Analytics can be broken up into 3 areas:
   i. Telemetry
   ii. Analysis
   iii. Actions

b. For telemetry, Analytics gathers information about the devices, locations, infrastructure, apps, and content accessed/modified through the different integrated services.
   i. This information is analyzed by the machine learning micro service to try and identify behavior patters for users, apps, and data. As behaviors are learned, the analysis engine can then spot anomalies or changes in behavior. Where is the user located? Is this a new/old device? Have they ever accessed this app before? Is this an unusual time for the user to access the app? Are they modifying a lot of files? Downloading content?
   ii. Changes in behavior or performance can automatically trigger an action, which can be something as minimal as an alert to the admin or more drastic like locking the user or wiping data from the device in question.
      - Monitor user behavior.
      - Detect anomalous activity.
      - Automate policy control.
      - Utilize multiple data sources.

Information from the different data sources are sent to Citrix Analytics service. Those are assessed based on policy-based violations, AI anomaly, user behavior modeling over time, or peer group normalization, and then the user score is created based on the aggregate level of risk a user poses to the organization.

Performance Analytics is a powerful tool to determine RCA that is causing poor end-user experience. It allows customers to quantify UX and app performance. It also gives customers the ability to have multisite aggregation and reporting.

The UX score is composed by getting information from an end user's latency, logon duration, failures, and reconnections. It allows you to drill down further to find the RCA of the issues your users are experiencing.

citrix™

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States