Solution Brief

Migrate to a VPN-less solution with Citrix Workspace

Enabling remote work for business continuity doesn't need to be reactive. By designing for remote work, you get continuity. The traditional VPN has been a key service for people doing their work while remote. But to enable people to continue to work remotely no matter what happens, it's extremely important that this service is highly available, secure, scalable, and performing well.

To meet these requirements for remote workers, Citrix provides a cloud-based, VPN-less solution to access all applications. IT can provide remote workers access to all intranet web, SaaS, mobile, and virtual applications, as well as physical PCs, without having to manage a VPN. Citrix Workspace provides a better alternative to VPNs because:

- **VPNs are complex to manage and scale.** They take too much time to configure correctly and policies can be too restrictive or too open.
- **VPNs don't provide an optimized user experience.** They are often clunky and restrict device choice. And they are too slow and consume a lot of bandwidth.
- **VPNs represent an old castle-and-moat model of security.** They are too risky to use for remote work use case in today's world, where many apps and data reside outside the datacenter.

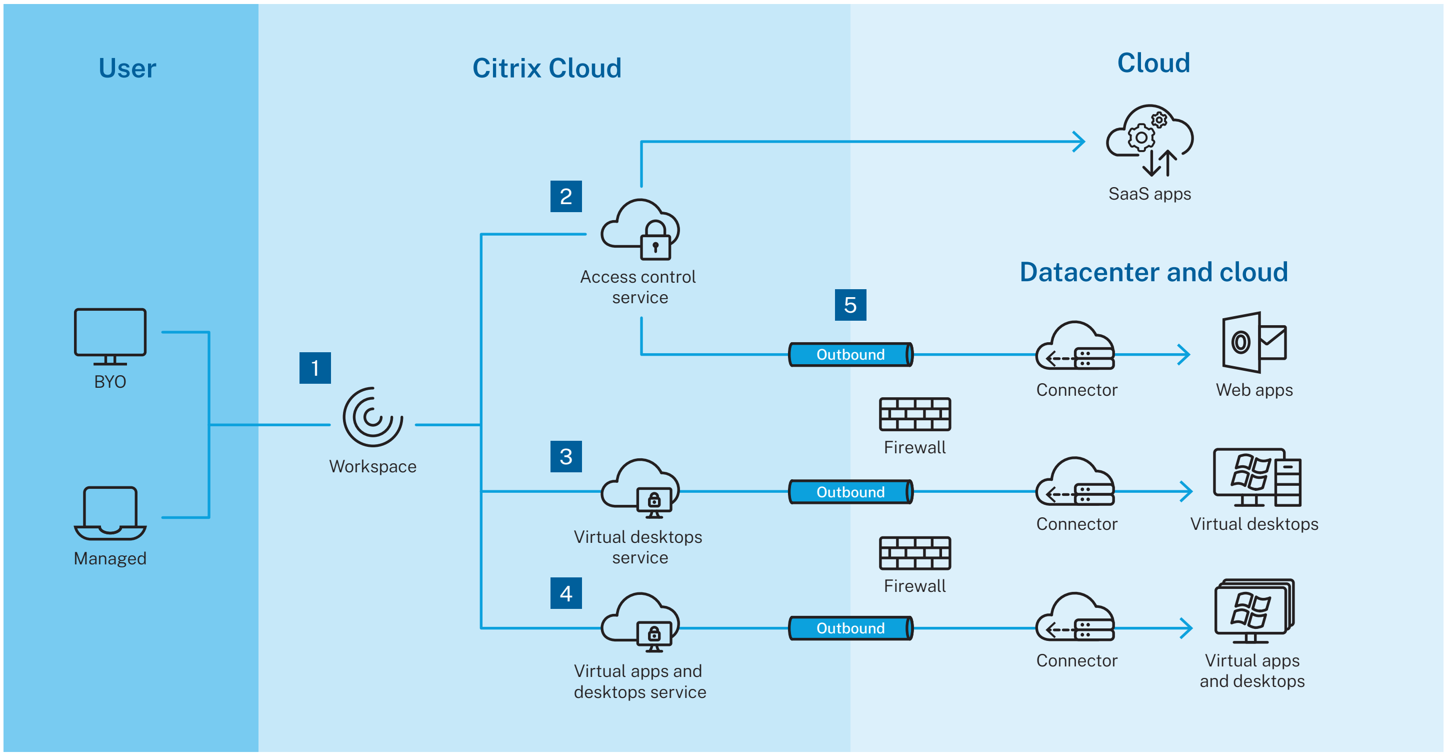
For most customers using a traditional VPN solution for remote access, Citrix recommends a phased parallel migration. A new infrastructure is built in parallel to the existing environment and allows organizations to onboard users and apps without modifying the existing infrastructure. The advantages of this approach are:

- The production environment is not affected.
- Testing is simple and isolated.
- Rolling back to a previous configuration is easy.

After you have decided the features you want to include in your deployment, you deploy Citrix Workspace infrastructure side by side with the existing infrastructure. Migrate users and whittle down one service at a time until you can officially retire your old VPN and no new employees get a VPN account by default.

The migration plan is split into four phases to provide a seamless transition:

- Design
- Deploy
- Migrate
- Retire



1 Choice of identity provider (AD, AAD, Okta, Google, Radius, and more)

2 VPN-less access with enhanced security to SaaS and web apps

3 VPN-less access to physical, Windows 10 PCs

4 VPN-less access with enhanced security to Windows and Linux apps and desktops

5 Outbound-only control channel provides resource specific access

Phase 1: Design

Create a plan before starting the migration. Citrix Workspace has a number of features that enrich the remote worker user experience.

1. Learn about Citrix Workspace

   a. Citrix Access Control combines the capabilities of instant secure access to SaaS and web applications through single sign-on (SSO), along with browser and cloud-based app controls, web-filtering policies, and integrated user-behavior analytics.

   b. Citrix Virtual Apps and Desktops gives IT control of virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device's operating system and interface. You should plan on delivering two-tier and local Windows and Linux applications using virtualization, as doing so will improve performance and security for these applications.

   c. Remote PC Access enables organizations to easily give employees access to their physical office PCs, rather than having employees carrying the PCs home.

   d. Citrix Content Collaboration unites all your data and documents in one secure platform—empowering employees to work better. Using this, you can keep a close check on sensitive information and how it is being used.

2. Plan the Citrix Workspace migration

   a. Decide which users and endpoints will be migrated first. Power users are great for providing feedback while testing.

   b. Infrastructure

      i. Sign up for Citrix Cloud

      ii. Decide which identity provider will be used: AD, AAD, Okta, Google, or Radius.

      iii. Decide where the Citrix Cloud connectors will be deployed.

   c. Determine which apps will be migrated in order from least to most complex

Phase 2: Deploy

Deploy a side-by-side VPN-less infrastructure starting with a subset of users able to test and provide feedback.

1. Deploy cloud connectors and VDA agents where needed and install workspace app on the endpoints.

2. Enumerate apps in order, from least to most complex:

   a. Web and SaaS apps are easily deployed first with Citrix Access Control. This is part of the Citrix Workspace solution and does not require virtualization. If you are an existing Citrix Workspace customer, you already have this entitlement.

   b. Two-tier client server apps often require more bandwidth and can perform poorly when delivered through a VPN connection. In addition to local Windows and Linux apps, you should certainly look at virtualizing traditional two-tier apps, as it improves their performance and provides granular security controls to access sensitive data within these applications.

   c. Desktops require additional configurations and preparation, such as provisioning and golden images. You employees need not carry physical desktops with them, but can use any device to access their physical desktop with a near-native experience as well as granular security controls.

3. Document the Citrix Workspace configuration

   a. Document configurations, IP addresses, and naming conventions.

   b. Develop runbooks or deployment guides for new administrators.

   c. Create training guides or videos for faster end-user adoption.

Phase 3: Migrate

1. Target service and endpoint migrations in steps to help identify any issues before they affect the entire organization.

2. Test the deployment and gather feedback with User Acceptance Testing (UAT). Use Citrix Performance Analytics to ensure two-tier apps and desktops are performing well with designated testers.

3. Make adjustments to configuration and apps as needed, and update documentation.

4. Add additional end users and departments until all have been migrated.

Phase 4: Retire

Properly decommission the legacy VPN environment after you have migrated everyone off.

1. Remove the legacy VPN configuration from endpoints.

2. Move users to new Active Directory groups as they are migrated successfully.

3. Decommission the legacy VPN server and remove configuration settings and DNS records.

Building an employee experience that enables remote work in a secure, consistent, and fulfilling way builds flexibility into the fabric of the organization. And while organizations can have many services behind VPNs, it's easy to migrate to Citrix Workspace and retire legacy VPNs. During this transition period, organizations can keep their VPN service up and running. Simply migrate services one by one, focus on the high-priority services first and work down until the last service is moved.

Get started today

Please refer our proof of concept guides on Citrix Access Control to get started.

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