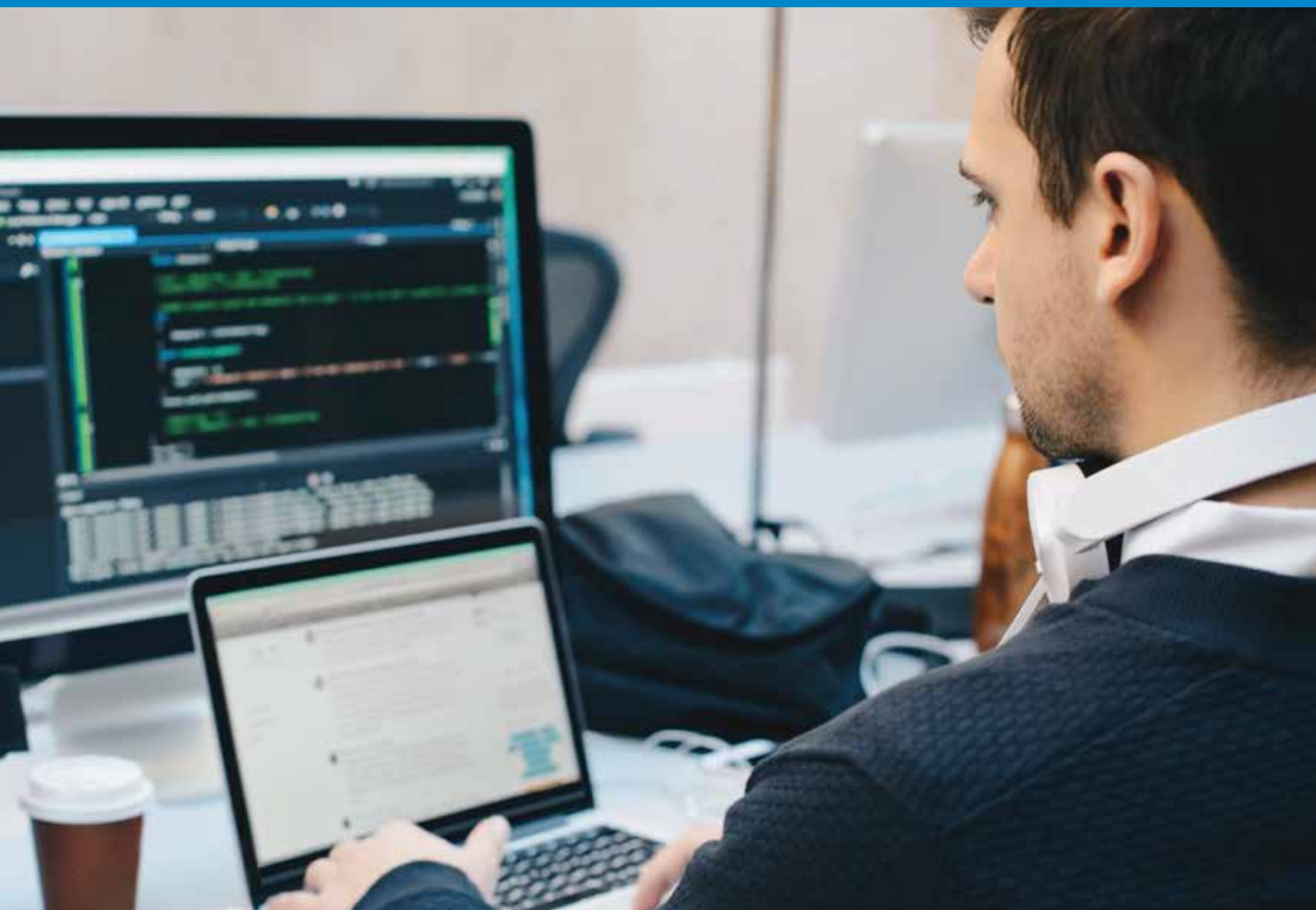
citrix

White Paper

Migrate to a VPN-less solution with Citrix Secure Private Access



The old castle and moat approach of delivering security forces the backhauling of all user and application traffic through an already congested datacenter network introducing latency, and not allowing security controls to be inforced in real-time.

As more users work remotely and applications continue to be deployed in the cloud, IT struggles with scaling and maintaining on-prem infrastructure, which eventually leads to poor performance and less than satisfactory end-user experience.

Also, with the increased use of BYOD, new threats are emerging. These threats are disrupting the organizations, leading to losses running into tens of millions of dollars.

A new approach with Zero Trust delivering security as a cloud service allows auto-scaling based on the user and IT requirements providing a more agile and effective way to reduce risk and deliver the best end-user experience. This approach allows security controls to be enforced in real-time and at the edge, which is closer to the applications and closer to the users, thereby reducing the risk from any external or internal threats.

Appliance-based solutions like VPNs and SWGs were designed for a very small percentage of employees working remotely, providing security for only a subset of applications. With working from home now becoming a norm, appliance-based solutions are hard to scale, require traffic to be backhauled, and separate login experience. IT is struggling to provide a solution that provides the best user experience and security.

Citrix Secure Private Access helps simplify IT, and provides a secure user experience irrespective of the user location or the device in use. As a cloud service, it is available across all GEO locations and scales automatically as the user count and usage increase, delivering agility and always-on security for the best user experience and security. Given it is a fully managed service, it allows IT to focus on more strategic initiatives as opposed to managing appliances across their datacenters. As an on-premises solution, Citrix Secure Private Access provides zero trust access to web and SaaS applications by leveraging NetScaler and Citrix StoreFront, as well as end-to-end visibility with Citrix Director.

For added security, Citrix Secure Private Access provides adaptive authentication policies and multi-factor authentication with continuous device posture assessment. Citrix Enterprise Browser works together with Citrix Secure Private Access as a secure web browser that allows your users to access internal web and SaaS apps while maintaining security and compliance.

Application access can be enabled based on user role, location, and device posture - Citrix Secure Private Access scan endpoints based on various factors such as anti-virus, OS, firewall, registries, and also allows for integrations with 3rd party solutions like Microsoft Intune or CrowdStrike.

As an example, a contractor on an unidentified device may be prompted for additional authentication steps, or an employee accessing an application from an unusual location may be denied access.

Why Citrix Secure Private Access provides a better alternative to VPNs.

- **Holistic, consolidated Zero Trust security strategy:** Citrix Secure Private Access enables IT to implement a holistic Zero Trust strategy across users, applications, files, and endpoints.
- **Zero Trust Network Access (ZTNA) to ALL private applications:** VPNs are challenging to scale, create privacy concerns, and don't meet today's modern security standards. Citrix Secure Private Access provides Zero Trust Network Access (ZTNA) to applications whether these applications are web, SaaS, TCP, UDP or VDI and virtual applications, and are deployed on-premises or on any public cloud delivering Zero Trust outcomes.
- **Adaptive authentication and Adaptive access policies:** Citrix Secure Private Access provides capabilities to scan end user devices before and after a user session is established. Based on the results of the user location, and the device posture assessment, an admin can define how they want to authenticate and authorize access to applications. These policies can be implemented for all applications, including for Citrix Virtual Applications and Desktop service.

- **Safely implement a BYOD program:** BYOD programs reduce device costs and management burden but introduce security risks, and the increase in remote work and the use of personal devices for work has created new security challenges. With no insight into device health, IT can't defend against common types of malware. Citrix Secure Private Access secures access from unmanaged devices by scrambling keystrokes and returning screenshots as blank screens, protecting sensitive corporate applications and data. Most people use consumer browsers on their personal devices, which can pose a risk to your enterprise resources. Citrix Enterprise Browser can be installed and fully controlled on BYO devices so that users can securely access enterprise applications without a corporate managed device.
- **Protection against web-borne threats:** Web access powers productivity but also enables attackers to distribute dangerous malware. Citrix Secure Private Access ensures users, devices, and networks stay protected against these threats. Consumer browsers are susceptible to attack, too. Citrix Enterprise Browser provides a solution for your users to securely access enterprise applications via an IT-managed browser. Additionally, for applications with sensitive content, an isolated (air-gapped) Remote Browser can be used for access.
- **Complete end to end monitoring of traffic across applications:** Citrix Secure Private Access offers complete end-to-end monitoring and visibility of all user traffic for all IT sanctioned applications. Having a single dashboard helps simplify monitoring as well as helps unify siloed environments.
- **Detect and defend against potential risk:** With insights into applications, files, devices, and networks, Citrix Analytics for Security helps automate security enforcements based on user behavior and anomalies detected in the system. This helps reduce manual work for IT, provides timely enforcement and reduce risk of unauthorized breaches.

For most customers using a traditional VPN for remote access, Citrix recommends a phased parallel migration. A new infrastructure is built parallel to the existing environment and allows organizations to onboard users and applications 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 on the features you want to include in your deployment, enable Citrix Secure Private Access side by side with the existing infrastructure. Migrate users and whittle down one service at a time until you can officially retire the 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

Phase 1: Design

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

1. Learn about Citrix

    a. Citrix Secure Private Access provides the capabilities of a VPN-less solution that delivers Zero Trust access with adaptive authentication and SSO to web, SaaS, client-based, and virtual applications through a unified portal. It provides security controls for managed, unmanaged and BYO endpoints thus giving end users device choice while improving the user experience by simplifying access to company resources.

    b. Citrix VDI/DaaS solutions 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.

        a. Plan the Citrix Workspace migration
        b. Decide which users and endpoints will be migrated first. Power users are great for providing feedback while testing.
        c. Infrastructure
            I. Sign up for Citrix Cloud
            II. Decide which identity provider will be used: AD, AAD, Okta, Google, or SAML.
            III. Decide where the Citrix Cloud connectors will be deployed.
        d. Determine which applications 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 the gateway connectors in your datacenter to allow secure, outbound only, connectivity.

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

    a. Web and SaaS applications are easily deployed first with Secure Private Access, without the need for agents or complex configuration. Additional per application DLP security controls can be applied to prevent data theft.
    b. Two-tier and legacy applications can then be delivered with agent-based Citrix Secure Private Access. Citrix Secure Private Access provides *Zero Trust Network Access* to IT sanctioned applications providing a secure hybrid work environment.
    c. A few two-tier applications may require intensive bandwidth and may require virtualization. You should look at virtualizing those applications, as it improves their performance and provides granular security controls to access sensitive data within these applications.
    d. Desktops require additional configurations and preparation, such as provisioning and golden images. Your 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 issues before they affect the entire organization.
2. Test the deployment and gather feedback with User Acceptance Testing (UAT).
3. Use Citrix Performance Analytics to ensure applications are performing well with designated testers.
4. Adjust configuration and applications as needed, and update documentation.
5. 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 Secure Private Access to get started.

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