citrix

Solution Brief

Why Citrix Workspace is a better choice than VPN for today's remote workforce

More people than ever are working remotely. Traditionally, a VPN has been the security solution of choice for providing secure access to corporate systems and files. But VPNs are complex to manage, and they introduce network-level security risks. They also provide a poor user experience, and are neither scalable nor privacy-friendly.

The old castle-and-moat security model of traditional VPNs has been surpassed by the strict principles of a zero trust framework, which contextualizes access based on request. Citrix Workspace provides a cloud-based, VPN-less solution to access all intranet web, SaaS, mobile, and virtual applications—whether using managed, unmanaged, or bring-your-own devices (BYOD) over any network. This solution brief explores why Citrix Workspace is a better choice than VPN to meet security, performance, and scalability requirements for remote workers.

VPNs are complex to manage

Depending on their role or the resource being accessed, remote workers are often given distinctly different access methods. An employee, administrator, partner, or vendor uses different login points within the same VPN. Multiple VPNs are typically required, and access to SaaS applications uses a different SSO portal. For system administrators, this is time consuming and can require significant resources to manage. Adding emergency capacity requires a forklift hardware upgrade or a drawn-out licensing procurement process.

VPNs often provide a binary option for access—full access or no access. They require the configuration of complex policies to prevent an unmanaged endpoint device from having unrestricted access to the network, resources, and data.

When you replace traditional VPN appliances with a fully managed, globally available, cloud-based service, complex network security policies are removed because you have provided contextual protected access to applications and data.

VPNs aren't designed for high-volume use

No matter where remote workers are located, they expect seamless access to the corporate network, and employers expect the same. However, with a VPN, all user traffic may traverse the corporate network, increasing congestion and reducing performance. Also, since it's common for a VPN to be deployed in a central location while users connect to internal web applications from geographically dispersed locations, the added latency degrades the end-user experience.

Remote workers can struggle when accessing traditional two-tier apps such as those used by billing and CRMs. These applications require a client on the end-user device, and the applications use native protocols with extensive bandwidth requirements that quickly overload VPNs and network pipes.

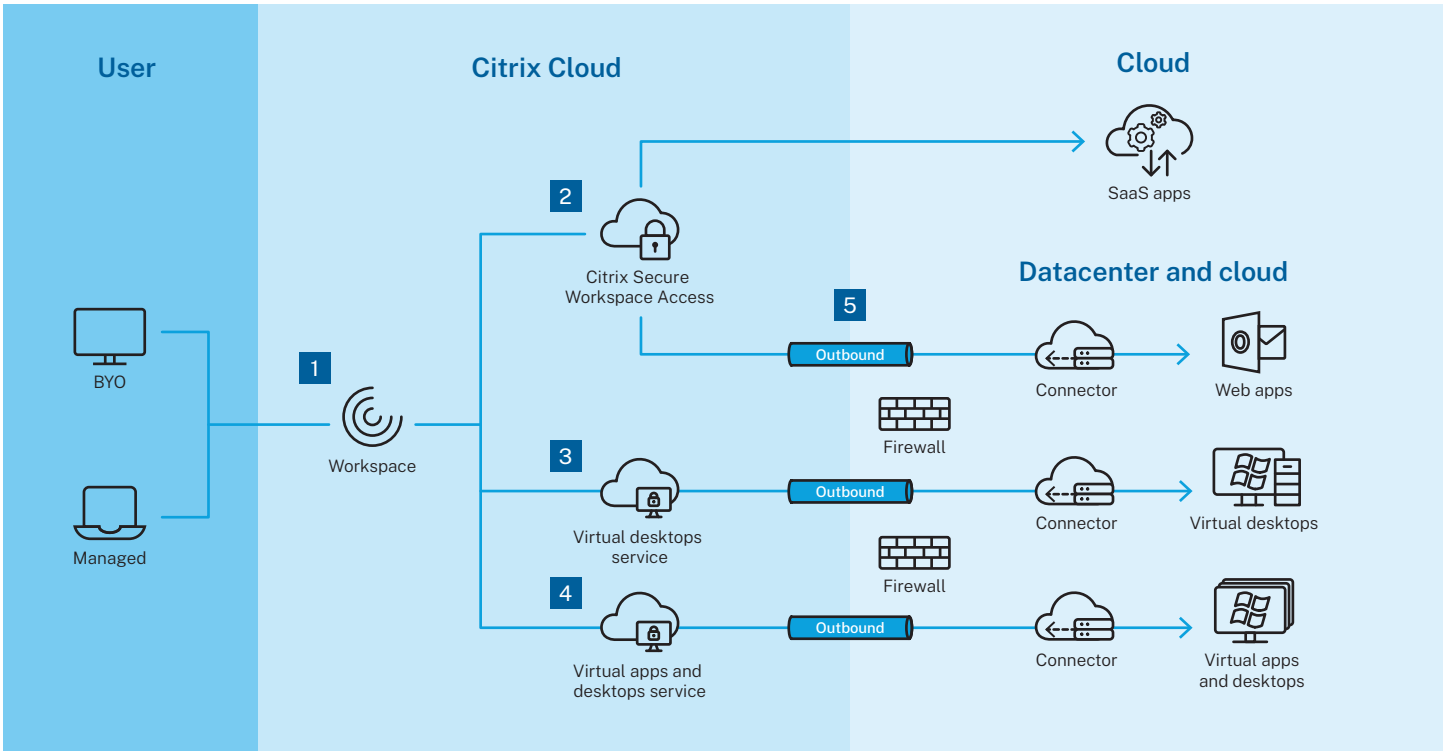
As network congestion and latency increase, the app responsiveness degrades, resulting in an inconsistent and sometimes unacceptable user experience. Suboptimal network conditions on the end user's side take performance and user experience out of your control.

Citrix Workspace gives your users VPN-less access to web apps

Citrix Secure Workspace Access service, part of Citrix Workspace, provides a VPN-less experience for applications that can be accessed using a browser. In this way, modern applications are delivered natively on any end-user device—with all of the contextual security controls in place—and they do not require any mode of network-level access.

Since Citrix Secure Workspace Access is available globally, a user is directed toward the nearest possible point of presence (POP) location. This ensures the best performance and security for accessing both SaaS and web applications.

For traditional two-tier applications, bandwidth can be a concern, and performance suffers when accessed from high-latency networks like home Wi-Fi. Delivering access through a virtualized platform not only improves the end-user experience but also provides granular security at the application layer. Citrix Virtual Apps and Desktops, part of Citrix Workspace, provides the best security and performance for these applications by minimizing the bandwidth requirements and dynamically adjusting both performance and security controls.



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

Citrix Virtual Apps and Desktops offers a better-than-native experience for remote workers. Apps that are chatty—network and computer intensive—are virtualized and optimized in the datacenter. The application client is also virtualized and runs near to the data source. The remote worker experiences an internet-optimized protocol which performs well even on congested networks.

VPNs compromise employee privacy

Security policies require network monitoring. If a VPN is configured to disable split tunneling, all the traffic, even to personal and private apps, will traverse the corporate network. You can observe non-work-related traffic, presenting considerable privacy concerns for remote workers using the device on their personal time. Remote workers are rightly concerned with the possibility of someone eavesdropping on their internet connection, gaining access to their computers and home network, or collecting data from the websites they visit.

On the other hand, when access ends at the application layer, workers feel that their privacy is secured. The end user is not subject to monitoring, and personal network traffic remains private.

VPNs can cause BYOD to put strain on IT teams and infrastructure

Recognizing the value in allowing workers to use their device of choice, many organizations are embracing BYOD initiatives. However, when remote workers connect to the network via VPN, ensuring the ongoing security updates, compliance, and compatibility of their devices can consume IT resources. That is the point at which a BYOD initiative stops reducing endpoint and access costs and puts enormous stress on IT infrastructure.

Many VPNs don't provide the contextual and granular security policies to support BYOD and unmanaged devices. Remote workers are required to have

a corporate-issued and managed device. Many organizations also use third-party companies to handle items such as payroll, benefits, and help desk support. Since autonomous third-party vendors have their own device setups, controlling and securing the endpoint becomes impossible.

In contrast, Citrix Workspace provides a rich user experience on any device through the Citrix Workspace app or a web browser.

Remote workers can require access to physical desktops from BYOD or personal devices. Citrix Remote PC Access allows an end user to log on to the physical Windows PC in the office from anywhere. And, for mobile devices, a per-app Micro-VPN capability further reduces the need for full VPN per-device connectivity. User experience is enhanced as the need to configure and launch a VPN client is removed, allowing for seamless access to secure corporate data.

VPNs open an all-access pass to your network

VPNs represent an old castle-and-moat security model in which access is all or nothing. You can't see or control who's accessing what. This makes it difficult to manage insider threats and stolen credentials.

VPNs increase the probability of network level security attacks when users need only application access. Even compromised endpoints can become participants on the network, leading to easy malware propagation.

Citrix Workspace is a secure, VPN-less solution for remote workers

Citrix offers a single, frustration-free remote work environment that solves your organization's security, management, and scalability challenges. Citrix Workspace aggregates all resources into a single, personalized user interface accessible from any device.

Regardless of the selected approach and the chosen device, remote workers access your apps, files, and data with a single-sign-on (SSO) experience without a VPN. Security is augmented with Citrix Secure Workspace Access service, which replaces traditional VPN appliances with a fully managed, globally available, cloud-based service. Complex network security policies are removed by providing protected access to applications and data.

Whether your workers are using virtual, web, or SaaS apps, Citrix Workspace determines the authorization rights based on conditional or contextual information that is user- and device-based. Contextual security policies allow you to not only identify and authenticate a user, but also to control what user actions are available within an application based on parameters such as user and device state, location, and IP address. Citrix Workspace also enables organizations to allow different levels of application or resource access. Only trusted users and devices are allowed to perform specific functions, such as clipboard cut and paste, printing, and local copies of files.

With the Citrix Secure Workspace Access service, you can add secure access controls and visibility to SaaS and web apps. App protection policies protect against keyloggers and screenshot malware. Watermarking protects access to sensitive applications and information. Rather than denying access to a remote worker connecting from on an untrusted device, you can restrict which functions the users can access.

For continuous monitoring and enforcement, Citrix Workspace gives security admins continuous user risk assessment and risk scoring. Mitigations are enforced to protect the business after initial login validation.

Benefits of Citrix Secure Workspace Access:

- Simple to deploy and configure
- Easy to manage and maintain
- Protects underlying network
- Protects end-user privacy
- Uses contextual or conditional access
- Provides a rich user experience
- Rapid scalability and provisioning
- High performance for remote workers
- Allows end-user device choice (BYOD)
- Continuous assurance and monitoring

Conclusion

Every organization needs to know its remote workers are connecting just as securely as on-premises workers, no matter where they are or what device they are using. Unlike traditional VPNs, Citrix Workspace provides the oversight and control you need.

To learn more about the features and benefits of Citrix Workspace, contact your sales representative or visit citrix.com/workspace.

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