Three signs it’s time to move to a digital workspace

How thinking beyond desktops can improve user productivity, empower IT, and keep your data safer
Not so long ago, a corporate or virtual desktop was all you needed to quickly onboard employees. As we move into the future, that’s no longer true. Three emerging trends are an indication that if you want to keep pace with your organization’s growing productivity requirements, it’s time to move to the secure digital workspace.

1. Growing mobile workforce
2. Modernization of apps
3. Disappearing security perimeter

Learn how thinking beyond desktops can help you improve user productivity, empower your IT organization to be more agile and better protect your company data.
1. A growing mobile workforce
Employees want to choose where and how they work. In fact, a Gallup research report suggests, 37% of employees would change jobs to have the ability to work where they want at least part of the time. The study also reveals that only 57% employees work in a similar location as their coworkers 100% of the time. Businesses now recognize the potential to increase productivity, agility and employee experience through remote work—whether at home, a client site, a hotel or a coffee shop. It’s up to IT to evolve accordingly.

While it’s possible to deliver virtual applications to a mobile workforce, there are other factors that make virtualization only more challenging – specifically modern apps.

2. Modernization of applications
Increasingly, applications are designed to work on any platform. Microsoft Office is a good example of modern applications as its applications can run on a number of different platforms including Windows 10, iOS, Android and Macintosh. In addition, Microsoft Office can be delivered as native apps or even as a SaaS service. Yet modern applications introduce new challenges. How do you secure and manage modern apps? For example, a traditional client management tool such as SCCM allows you to deliver and manage legacy Windows desktop applications on a Windows 7 laptop, but it doesn’t allow you to manage Windows 10 modern apps on a BYOD smartphone and separate the employee’s personal data from company data. As a result, traditional client management tools are having to be supplemented with Enterprise Mobility Management. This combination of client management and Enterprise Mobility Management is referred to as unified endpoint management (UEM).

3. Disappearing digital security perimeter
With a more mobile workforce, company data increasingly becomes more difficult to retain in data centers. Your users need access to their files regardless of whether those files are located on servers behind your firewall, on a server hosted by a trusted provider, or on their desktop in the office. Some of your users may have resorted to using native mobile email clients as opposed to virtual mail, storing email file attachments on their personal smartphone in an un-encrypted format. At the same time, that employee may also be using a VPN which a hacker can use to access to your resources behind your firewall through a compromised mobile app your employee downloaded.

Did you know?

Over 1/3 of employees would change jobs to have greater flexibility?

Only 57% work in a similar location as their coworkers 100% of the time.
Go beyond virtualization and embrace a digital workspace with Citrix

A complete and integrated digital workspace will enable people to securely access their apps, desktops and data from anywhere. Citrix Workspace suite combines virtualization technology with other capabilities including unified endpoint management (UEM), enterprise file sync and share (EFSS), secure network access gateway and Analytics for intelligent security and application performance monitoring.

Unified endpoint management

Citrix Endpoint Management, using technology formerly called XenMobile, makes it easier for IT organizations to manage their growing mobile workspace. The solution provides centralized management across a number of different platforms and devices including desktops, laptops, smartphones, tablets, IoT devices and other thin clients such as Google Chromebook. In addition, Citrix allows you to manage not just mobile apps, but modern apps. Also, Citrix Endpoint Management exclusively provides unique capabilities that add value to Microsoft EMS/Intune including micro-VPN for O365. You’ll be able to keep data on mobile devices encrypted, reducing the problem of a disappearing digital security perimeter.

Unified endpoint management features:

• Mobile device management (MDM) across popular platforms (including Windows 10, iOS, Android, MacOS and IoT)

• Flexible mobile application management (MAM) with support for platform MAM (such as iOS managed application, Samsung KNOX, AppConfig Community, Windows Information Protection); Citrix MAM with MDX technology that provides a second level of application level encryption without device enrollment; and support for Intune MAM to protect O365

• Enterprise-grade, secure productivity apps including Citrix Secure Mail and Citrix Secure Web.

• Mobile content management (MCM) including Citrix Content Collaboration technology integrates with Secure Mail which allows your employees to access work files anywhere with a click of a link in their email and eliminates the need for users to send email attachments

• Identity management (IDM) with support for 2-factor authentication and SSO for any app (mobile, virtual, SaaS, Web) delivered through a customizable app store

• Network gateway access security with unique micro-app VPN, which reduces the risk of unauthorized access to your network

Citrix Content Collaboration

While app and desktop virtualization does allow users to access their files from virtual apps, as noted earlier, more users are adopting modern apps, and therefore, need a comprehensive, secure solution to access their files regardless of the type of app and regardless of where their apps might be stored. Content Collaboration from Citrix complements app and desktop virtualization as part of a complete digital workspace.

Content Collaboration from Citrix provides:

• Anywhere, any-device data access through data sync tools and apps

• Secure access to data within the network including SharePoint and network drives

• A seamless, convenient user experience with Microsoft Outlook® Plug-In, Windows Explorer and Mac Finder Integration; Large File support—up to 100 GB; Built-in Mobile Content Editor

• Control over where data resides through storage zones and connectors for SharePoint and network drives, giving IT the flexibility and control to store data wherever best fits requirements of regulatory compliance, IT strategy and infrastructure.
• Centralized management and security, including robust reporting and notification features and DLP integration

• Native device security policies to extend security to endpoints

• On-demand sync for virtual desktops

**Citrix Gateway**

With more types of devices and apps being used, remote access can easily become much more complex for IT, with a myriad of more point products for different devices, ownership models, networks and apps. IT needs to consolidate and simplify remote access infrastructure while giving people simple, access their apps from any device.

Citrix Gateway provides remote access from any device type to virtual environments; SSL VPN-based remote access to enterprise apps, web apps and SaaS; and integration with Citrix Endpoint Management for secure mobile device access.

**Citrix Gateway also provides:**

• One URL to access any app using any type of device providing unified, secure access

• Micro-VPN capabilities for secure mobile device access

• A stable, high-performance app experience over any network

• Single sign-on (SSO) to virtual, mobile, web and SaaS applications

• Multi-factor authentication, end-to-end monitoring across all application traffic and context access control

**Citrix Analytics**

By employing a wide set of machine learning algorithms, Citrix Analytics delivers contextual security: it correlates and analyzes cross-product data to detect and isolate risky user activities, whether they stem from an internal employee or malicious external attacker.

These risky user activities are combined to create an aggregate risk profile for the user. Once risky user activities are identified, Citrix Analytics employs a variety of granular policy controls to mitigate the threat or stop it entirely: enabling multi-factor authentication, recording user sessions, setting tighter data access thresholds, blocking suspicious apps and even quarantining users to name a few.

**Citrix Analytics provides:**

• Security Analytics based on user behavior combining access security analytics, application security analytics, and data security analytics

• Performance and operations analytics to track usage, monitor performance and highlight issues and root cause

• Operates in real-time closed loop by modifying product policies to mitigate threats

• Works on premises, in a public cloud or hybrid deployments
Where to begin

Many Citrix customers approach the move to a digital workspace through a phased implementation focusing on user personas and use cases for their mobile workforce. You’ll also need to identify key use cases and workflows. Consider these from the perspective of users and the workforce, and their needs, preferences and workstyles across different types of devices, apps and networks. Your assessment should also include business requirements around security and compliance. Many of these use cases might be tied to current projects such as Windows 10 migration or O365 adoption.

Next, create a conceptual solution mapping out the proposed user experience and workflows. Focus initially on low-hanging fruit that can deliver quick wins such as adopting Citrix Endpoint Management to manage Windows 10 devices and modern applications along with management for other devices and apps. Or add Citrix Content Collaboration to support important file sharing use to reduce data loss.

Your proof-of-concept should include representatives from all business units to ensure that you’re meeting the full spectrum of requirements. Implement your solution either on-premises, in the cloud, or hybrid in phases based on your users and use cases you identified.

Conclusion

The rise of mobile workstyles, modern applications and a disappearing digital perimeter, poses challenges that can’t be addressed through virtualization or a piece-meal, multi-vendor technology stack. Only a complete and unified workspace solution can empower people to be fully productive on any device, using any app, with the high-quality experience they demand and the security IT requires.

A workspace complete with full mobility support lets IT streamline and simplify. Working with a single vendor for a complete digital workspace saves time, reduces staff training needs, simplifies technical support, lowers overall costs and gives users a more seamless and convenient experience. To improve employee engagement and productivity, the employee needs a digital workspace that is context aware, reliable, and intelligent enough to offer up the right access, the right insight, and the right performance to get the job done.

With Citrix Workspace, organizations can overcome headaches around security and management, provide a rich set of enterprise-grade mobile productivity apps, enable secure file sharing on any device and deliver a seamless experience through a single, comprehensive solution. By implementing Citrix Workspace through a phased approach based on your most important use cases, you can complete the transition to a digital workspace delivery while driving optimal value for your business.

Sources

1 Gallup: State of the American Workplace, 2017