No enterprise can expect to compete effectively without embracing mobile technology and the capabilities it provides for workers to better perform and meet the expectations of customers. Fully realizing the potential of mobile requires adoption of an enterprise mobile management strategy based on a secure, enterprise mobile device management (MDM) architecture that provides role-based management, configuration and security of corporate and user-owned “Bring Your Own Device” systems.

Clearly, mobile technologies have taken the enterprise by storm. In CIO magazine’s 2013 “State of the CIO” survey, 38% of respondents indicated they had completed or planned mobility initiatives in 2012, and 52% anticipated such initiatives in 2013.

In a survey commissioned by Citrix, 1,900 senior IT decision makers from 19 countries were polled in the second half 2012. The findings indicated that organizations that have implemented mobile work styles will rise from 24% in 2012 to 83% in 2014.

In that survey, the average number of devices connecting to the corporate network in 2012 was 5.18 per knowledge worker, and two-thirds of those polled said their organizations permit if not encourage BYOD environments that allow employees to work and connect to enterprise networks using their own devices.

But it’s not just a matter of using personal devices to access enterprise email. Workers increasingly want access to Windows, data center, Web and native mobile apps that will allow them to perform their jobs no matter their location. Naturally, for IT that raises significant security and compliance concerns. That can put IT in a situation of either imposing rigid controls over the environment, or acquiescing to user demands without a clear strategy for how to deal with security and management issues.

With executives, workers and lines of business all clamoring for speedy access to mobile solutions, IT has to reconcile how it manages mobile devices, apps and data in a secure, compliant manner while providing users the freedom to experience work and life their way.

**Mobile Device Management**

Typically, organizations respond to mobility demands by requiring people to use different devices for different activities or securing and managing devices, apps and data with a complex array of point solutions. One approach frustrates users and exacerbates tensions between IT and the business while the other fosters management and security headaches.
Attempting to buy and then cobble together point solutions into an effective enterprise mobility management architecture is time-consuming and inefficient.

What is needed is a comprehensive, flexible solution to manage mobile devices, apps and data. Such a solution must prevent data loss and protect against mobile threats while enabling BYOD and supporting customers.

The ideal MDM architecture will encompass secure email, documents, collaboration, support, legacy apps and an app ecosystem. The architecture must also provide tight integration with Web apps, Windows apps and desktops, as well as a company’s network enterprise directory system. It should enforce tight control across the entire device lifecycle by:

> Configuring device settings and policies, such as device and application restrictions
> Provisioning devices via self-service enrollment and centralized distribution of configurations, policy and application packages and updates
> Securing devices, applications, the network and data with authentication and access policies, application and cloud service blacklisting and whitelisting, enforcement of secure application tunneling and deployment of content- and context-aware mobile data loss prevention policies
> Separating corporate apps and data from personal apps and data on the user’s mobile device through the use of container technology
> Monitoring devices, infrastructure, service levels and telecom expenses
> Supporting users with remote user device control and troubleshooting, along with the ability to remotely locate, lock and wipe devices in the event of loss or theft
> Decommissioning devices by identifying the ones that are inactive and wiping or selectively wiping them upon employee departure. With selective wipe, the corporate profile and all associated applications, including email, are removed without affecting the user’s personal applications and information.

Migrating from Legacy Desktops

Nobody leaps overnight from a legacy desktop application environment to one that is fully mobile. Some strategic issues, such as cloud use, are still taking form. It also may take time to create enterprise-ready mobile versions or alternatives of desktop apps that users need to be fully productive.

For businesses, however, new processes and management tools are required for provisioning, managing and securing all of these new applications. Organizations need to strike a delicate balance between empowering mobile users with the capabilities they need to stay productive, and protecting themselves from the multiple risks that personal devices and applications pose to network security and sensitive intellectual property.

The number of device-native email clients, and the different operating systems they are running on, represent a daunting challenge to IT. Each such app must be tracked and constantly monitored for updates and security patches. Depending on the client, users may have to, or simply be allowed to, mix corporate and personal email in the same account.

Limitations of Native and Web-based Apps

Native email client software is often open to sharing information with other applications and functions on the device, which adds the risk that corporate contacts, email and calendar entries could be accessed by other applications, including potentially malicious software. Other users may opt for browser-based Web mail, but unsecured Web browsers also bring their own risks, such as Web-based malware.
Virtual email is one of the most secure alternatives to native clients and browser-based mail, since applications and data are stored securely, either in the data center or locally in an encrypted file system with powerful enterprise policy enforcement. Another option is specialized sandboxed email client software such as Citrix WorxMail, which encrypts work information and keeps work-related applications and information unavailable to personal applications.

Once they have access to email on their mobile devices, many workers also expect to be able to access files and other data they consider vital to doing their jobs. File-sharing and synchronization cloud services such as Box, Dropbox and Google Drive are easy to use and easy to subscribe to, but these services were created for consumer use, not the security-conscious enterprise, and pose their own risks. Since information is stored in the public cloud it is difficult or impossible for IT to exert any control over which information is stored in which account or to wipe sensitive information or block access when users change roles or leave the organization.

### Bridging Mobile Worlds

Enterprises are straddling two worlds today—Windows apps and non-Windows apps. Previously the primary business applications, Windows apps are now just one of four major app types. So while IT is supporting business-critical, legacy Windows apps and eliminating noncritical ones, it must also now support a variety of non-Windows apps as organizations move to mobile environments. The three major non-Windows apps are: native client apps, Web-based and SaaS apps, such as Evernote, SAP and Salesforce.com.

Employees may be using multiple devices during the course of a day, including desktops, laptops, tablets and smartphones, often using different app types to accomplish the same tasks on those different platforms. Many workers will still require access to the productivity tools provided by legacy and Windows desktop applications, while others may be served by approved native mobile apps or Web apps.

IT organizations need a strategy to determine whether and how they will carry forward legacy Windows-based business processes to new platforms while accommodating user trends and demands for faster access to the devices of their choice.

There are different strategies to provide workers with the needed mobile apps, and most organizations will likely employ some combination of the following:

- **Build native applications** for iOS, Android and Windows 8
- **Redesign existing apps** to take advantage of Windows 8 features
- **Build Web applications** with HTML5 and JavaScript
- **Create** hybrid native/Web apps
- **Mobilize** existing Windows application code

The challenge for IT is how to manage such a diverse environment and meet growing needs for collaboration and data sharing, network management, as well as desktop and application virtualization. Citrix has responded with a mobile enterprise management portfolio that incorporates MDM, a unified app store, secure access to business resources, enterprise mobility management, Windows apps and desktop virtualization, file sharing, collaboration and remote support:

- **Citrix XenDesktop** delivers Windows desktops as an on-demand service to any device, regardless of OS, and Citrix Receiver is a universal thin client that runs on virtually any mobile operating platform. These optimization technologies touch-enable crucial Windows apps, making them more usable on a mobile device without any source code changes. Employees gain single-click secure access to all of their Windows, Web, SaaS and mobile apps through a unified app store on any device, over any network, with single sign-on and seamless session roaming across locations, networks and devices.
> **A Citrix Mobile SDK** for Windows apps provides a rich toolkit for enterprise Windows/.NET developers to mobilize existing line-of-business Windows applications or write new touch-friendly, mobilized applications that are hosted on Citrix XenApp or XenDesktop and delivered to any mobile device with Citrix Receiver.

> **Citrix XenMobile MDM Edition** provides role-based management, configuration and security of corporate and user-owned devices, all running on a secure, enterprise MDM architecture. XenMobile MDM Edition lets administrators configure both corporate device and BYOD settings and integrate with IT resources in a centralized, role-based manner integrated with enterprise directories like Microsoft Active Directory. XenMobile enables users to self-service enroll, select apps from an app catalog and perform some self-help functions. Administrators can provision policies and apps automatically over-the-air to users.

> **Citrix Worx Mobile Apps** provides a gallery of mobile apps from Citrix and app development partners that are ready for use with XenMobile, including WorxMail for secure email, calendar and contacts; WorxWeb for secure Web browsing; and Citrix ShareFile for secure document sharing, sync and editing. The Worx App SDK enables third parties and enterprise developers to Worx enable their mobile apps, leveraging the Citrix MDX app container technology to add features like data encryption, password authentication, secure lock and wipe, inter-app policies and micro VPNs to any mobile app.

> **Citrix NetScaler** is a Web application delivery solution that maximizes the performance and availability of all applications and data by optimizing, securing and controlling the delivery of all enterprise and cloud services. The solution also maximizes the end-user experience for all users including mobile clients. NetScaler provides a single point of management for access control, auditing and reporting, support compliance and data protection.

### The Mobile End Game—Transforming Business, Transforming IT

The consumerization of IT will continue to drive the transformation of business and IT models in the coming years. People expect to use the latest mobile devices and apps because they offer great experiences and enable them to do what really matters when it matters most.

This user-driven, self-service approach to technology adoption is fundamentally changing how people, IT and businesses operate, collaborate and innovate. By embracing this trend, organizations can improve productivity, satisfaction, talent recruitment and employee retention.

The mobile transformation is occurring simultaneously with the rethinking of networking strategy and infrastructure to take advantage of cloud technology and deliver IT as secure, on-demand services. The cloud-based service delivery network supports all applications and services—regardless of where they originate and where they are consumed. The cloud will accommodate enterprise apps, cloud services, virtual desktops and mobile services.

The outcome of this transformation is new levels of productivity, but it requires new ways of thinking and adaptability in a volatile and unpredictable world. Citrix is helping organizations of all sizes adopt mobile work styles through a complete portfolio of market-leading cloud solutions that accelerate the path to IT-as-a-service.

With Citrix solutions, organizations can build, deploy and manage next-generation IT infrastructure and cloud services to deliver simple access to apps, desktops and data from any device over any network, with the best performance and reliability.

Enterprises can provide mobility with advanced management control and security for all apps and data on corporate and personal mobile devices. For more information, go to [URL landing page](#).