Enabling mobile workstyles with an end-to-end enterprise mobility management solution.
The evolution of mobile workstyles has made it increasingly important for professionals to be equally as productive on the go as they are in the office. The consumerization of IT is fueled by employee mobility, but also creates complexity for enterprise IT. Bring your own device (BYOD) programs, application proliferation, and consumer file-sharing services are leading to a mix of devices, applications and data that are difficult to control, secure and manage. By powering mobile workstyles with an end-to-end enterprise mobility management solution that includes Citrix XenMobile, Citrix Worx Home, and Citrix ShareFile, Citrix is helping to bring order out of this chaos.

**Consumerization of IT**
Professionals’ technology choices are becoming increasingly personal and represent one of many factors driving the consumerization of IT in the enterprise. With the force of this momentum, it is clear that in most business scenarios, users will continue to win the battle of choice for devices, applications, and services. Although there will be exceptions, heterogeneity is here to stay and will be adopted by CIOs as they look to make users as productive on-the-go as in the office.

Enabling highly productive mobile workers is a visionary goal, but embracing consumerization as an IT strategy presents significant practical challenges because it creates a broad mix of devices, applications, and data. The following sections present a closer look at the chaos cause by consumerization.
Device chaos

The ever-increasing range of devices and device platforms that fall under BYOD strategies can create chaos within the enterprise. To avoid it, a simple method is needed to rapidly connect personal and corporate devices to corporate infrastructure, enable users to engage efficiently with the required enterprise applications and data and apply appropriate security controls to devices that employees use for work.

Multiple factors influence accessing enterprise IT resources, such as device ownership, user role or status and current location. For example, the resources a contract employee can access from a personal device connected via a public WIFI network should be markedly different from the resources accessible to a permanent employee using a desktop PC on the corporate LAN. For compliance and manageability, IT must be able to configure devices as well as apply policies and actions such as passcodes, app blacklist/whitelist and full or selective wipe of lost devices. A flexible, policy-driven infrastructure that can cope with diversity of devices is critical to managing and securing the IT environment while enabling employee productivity.

User experience is also affected by variations in device platforms and form factors. The challenge is to provide a consistently rich experience on all device platforms including Apple iOS, Android, RIM, and Microsoft Windows, as well as on devices with different screen sizes and resolutions. To empower employees with full productivity while still ensuring the security of corporate applications and data, IT needs a way to manage devices throughout their entire lifecycle.
Application Chaos
The ever-growing mix of mobile, SaaS and Windows applications within enterprises is creating application management and support chaos. With the need to manage all these applications through their entire lifecycle and across a much broader range of devices, challenges abound irrespective of the enterprise application strategy.

Organizations embracing native mobile applications suffer from the inefficiencies of developing multiple versions for multiple platforms, as well as the security risks associated with distribution to unsecured devices. Adapting a large base of legacy desktop applications to be suitable for smaller, touch-driven interfaces operating over low-bandwidth, high-latency links is a time-consuming and risky proposition, as not all apps will work well in this new environment. Web applications present their own challenges, notably browser incompatibility and security. Personal apps that users download also present a risk as users may simply mishandle corporate data in these apps or have downloaded a malicious application onto the device.

With so many options available, application sprawl is a real problem for IT in terms of manageability and updates as well as security. Current trends are heading away from centralized IT licensing of apps and towards the purchase of SaaS services by departments for line-of-business needs. This trend anticipates more situations where individual applications are brought into the enterprise as a result of BYOD. These trends will create a new wave of application sprawl if steps are not taken to deliver all app types via a unified infrastructure.

Data Chaos
The exponential growth of data in the cloud and on devices is creating data management and security chaos. Data chaos occurs at the intersection of access, control, and security. The enterprise needs to make its data available to users while controlling and securing distribution to protect its intellectual property and meet regulatory guidelines regarding user privacy and auditing requirements.

The challenges of controlling and securing data arise from multiple, uncontrolled endpoint devices, poorly written and/or malicious applications and readily available consumer data-sharing applications. Also, when it comes to information security attacks, the biggest threats originate within the organization. These attacks are not necessarily malicious and may occur passively through poorly secured devices with no device PINs or data encryption and poor physical access protection. But, with the number of personal devices in the enterprises and cloud data services available, a fine-grained data policy that follows the users between devices becomes a necessity.

Citrix enterprise mobility management
Citrix offers a solution for controlling all three aspects of chaos with an end-to-end enterprise mobility management solution. XenMobile features mobile device management; mobile app management; sandboxed productivity apps; a unified corporate app store and multi-factor single sign-on. XenMobile also provides flexible deployment options for IT admins, with an offering on-premise or in the cloud.
Citrix XenMobile

Citrix XenMobile is a comprehensive solution to manage mobile devices, apps, and data. Users have single-click access to all of their mobile, SaaS and Windows apps from a unified corporate app store, including seamlessly-integrated email, browser, data sharing and support apps. IT gains control over mobile devices with full configuration, security, provisioning and support capabilities. In addition, XenMobile securely delivers Worx Mobile Apps, mobile apps built for businesses using the Worx App SDK and found through the Worx App Gallery. With XenMobile, IT can meet their compliance and control needs while users get the freedom to experience work and life their way.

XenMobile delivers the following key features:

**Configure, secure, provision and support mobile devices with MDM.** XenMobile delivers enterprise grade MDM with role-based management, configuration, security and support for corporate and employee-owned devices. Users enroll their devices, enabling IT to provision policies and apps to those devices automatically, blacklist or whitelist apps, detect and protect against jailbroken devices, troubleshoot device and app issues, and wipe or selectively wipe a device that is lost, stolen or out of compliance. Users can use any device they choose, while IT can ensure compliance of corporate assets and secure corporate content on the device.

**Mobile app management with the largest ecosystem of apps built for business.** XenMobile securely delivers Worx Mobile Apps, the industry’s largest collection of apps built for business. Developers leverage the Worx App SDK, a simple and powerful SDK that provides critical enterprise features into any app. The SDK leverages Citrix MDX app container technology to add features like data encryption, password authentication, secure lock and wipe, inter-app policies and micro VPNs to mobile apps. It comes with a library that can be embedded into any app with a single line of code. Developers can also opt to wrap their apps post-development without adding any code to their app. IT can find Worx-enabled apps in the Worx App Gallery and deliver these apps to devices via XenMobile. ISVs can use Worx App Gallery to promote their apps.

**Sandboxed email, browser and data sharing apps.** With XenMobile, IT can deliver Citrix-developed apps that are built for business. These apps include WorxMail for secure email, calendar and contact access, WorxWeb for a secure internet and Intranet access and ShareFile for secure enterprise file synchronization and sharing. WorxMail, WorxWeb and ShareFile integration deliver a rich user experience with the management and control that IT requires. These apps take advantage of capabilities in the Citrix Worx App SDK such as an app-specific VPN for secure access and a common data platform that ensures corporate data is encrypted and always under IT control.

**Unified corporate app store.** XenMobile includes a unified corporate app store that provides a single place for users to access all of their apps – mobile, web, SaaS, and Windows – on any device. Users can easily choose the apps they need for their job and have them instantly available on their devices. As they move among their favorite devices, their chosen apps follow them to ensure full productivity in any scenario.
Multi-factor single sign-on. XenMobile makes it easy for IT to manage user access and radically simplify the user experience. Through the unified corporate app store, users are given secure multi-factor single sign-on across their mobile, web and Windows apps ensuring that they don’t need to remember yet-another-password.

![Citrix Worx Home](logo) | [Citrix XenMobile](logo) | [Citrix ShareFile Enterprise](logo)
---|---|---
| Any device | Any device, app & data | Enterprise data |
PC | Mobile devices | Security |
Mac | Mobile apps | Account control |
Smartphone | Datacenter apps | Provisioning |
Tablet | Web apps | Follow-me-data |
Thin client | Windows apps | Access policies |
| Data | |

Figure 2: A complete enterprise mobility management solution

Worx Home
Available for any mobile device, Worx Home is an app that allows IT to enforce mobile settings and security while also providing access to a unified app store and live support services. XenMobile communicates with Worx Home to deliver device-specific policies and Worx-enabled app policies.

ShareFile
ShareFile underpins the data capabilities of XenMobile, giving users the ability to access and share their data from any device or location. ShareFile data is secured on mobile devices using remote data wipe and lock as well as device-based data access policies. In the following diagram, it is the “Data” component to the XenMobile App Controller.

NetScaler
NetScaler is a secure application and data access solution that provides administrators granular application and data-level control while empowering users with remote access from anywhere. It gives IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device, providing better application security, data protection, and compliance management.
Citrix XenMobile deployment model

Figure 3: Citrix XenMobile Architecture

XenMobile consists of three backend components: XenMobile App Controller, XenMobile Device Manager, and NetScaler. Together, these components address the challenges of device, application, and data chaos that enterprise IT faces from the consumerization of IT.

Managing Devices
The XenMobile Device Manager allows IT to manage devices throughout their entire lifecycle with enterprise MDM capabilities. These components allow IT to configure, provision, secure, support, monitor, and decommission any device—BYO or corporate-issued.

Managing Applications
XenMobile App Controller enables IT to ‘wrap’ any type of app and deliver it to employees through Worx Home, based on their role in an organization. Wrapped apps allow IT admins to place policies and controls over them, ensuring that corporate content stays safe and employees don’t inadvertently leak sensitive information. Citrix MDX technologies secure the apps that are delivered, allowing IT to apply security policies and encryption on application and data access.

Managing Data
XenMobile includes ShareFile, allowing IT admins to directly provision and manage ShareFile accounts through the App Controller interface. This provides employees instant access to their ShareFile Enterprise accounts, allowing them to securely access, edit, sync and share files from any device.
Conclusion

By resolving the device, application and data chaos created by consumerization, Citrix is enabling mobile workstyles for users while providing IT with control and management capabilities. XenMobile with Worx Home and ShareFile enables quick and effective access to the enterprise resources people need to stay productive on the go from any device, while supporting IT efficiency, information security and regulatory compliance.