10 essential elements for a secure enterprise mobility strategy

Best practices for protecting sensitive business information while making people productive from anywhere

CITRIX®

citrix.com/secure

Mobility and bring-your-own device (BYOD) are transforming the way people work and the way organizations support them. There's more to mobility than simply enabling remote access—and mobile devices are far more than limited-use gadgets. Capable of accessing, storing and transmitting applications and data like traditional computers, smartphones and tablets can be used for almost any business task. To unlock the full potential of enterprise mobility, IT needs to allow people the freedom to access all their apps and data from any device, seamlessly and conveniently.

Mobile devices also call for the right approach to security to protect business information even as they're used in more places, often over untrusted networks, with a significant potential for loss or theft. IT has to maintain compliance and protect sensitive information wherever and however it's used and stored—even when business and personal apps live side-by-side on the same device. Emerging mobile trends from wearable technologies to the Internet of Things are already raising new points to consider. Developing a truly comprehensive and security-conscious mobility strategy is now a top priority for every organization.

This paper presents 10 key points to consider as you develop your enterprise mobility strategy, encompassing security, user experience, IT operations and BYOD. As the leader in mobile workstyles, Citrix provides a complete solution to enable secure enterprise mobility, including technologies for mobile device management (MDM), mobile application management (MAM), application and desktop virtualization, and end-to-end security from datacenter to device. Together, these guidelines, best practices and technologies will help your organization realize the full benefits of mobility.

1. Manage and protect what matters

As people access data and apps on multiple devices—including personally-owned smartphones and tablets—it's no longer realistic for IT to control and manage every aspect of the environment. Instead, you should focus on what matters most for your organization, and choose the mobility management models that make the most sense for your business and your mobile use cases. There are four models to choose from, either individually or in combination.

Mobile device management (MDM) – MDM lets you manage and control mobile devices used to access business resources. Before a device—corporate-owned or personally-owned—accesses the enterprise network, you can verify that it hasn't been jailbroken or otherwise compromised. Encryption, remote lock and wipe, mobile VPN, app blacklists and the ability to selectively disable native device capabilities enable a high level of security.

Mobile hypervisors and containers – Especially useful to support BYOD, this model lets you manage apps, data, policies and settings within a container on the device without interacting with any personal content it may hold. In effect, a single mobile device becomes two separate virtual devices: one for work, and one for personal life.

Mobile application management (MAM) – Building on the containerization approach, MAM lets you centralize management, security and control for any mobile app as well as its data and settings as part of a container. App-level policies can include authentication, network, location, passcodes and encryption.

Application and desktop virtualization – The inherent security of virtualization applies in mobile use cases as well. Enterprise applications can be optimized for mobile devices and delivered on-demand while data stays protected within the datacenter.

2. Think "user experience" first

Mobile devices have been a key driver of consumerization in the enterprise, giving people powerful new ways to work with apps and information in their personal lives. This has raised the stakes for IT, which must now provide an experience that compares favorably with the freedom and convenience allowed by consumer technology companies. It can be helpful to sit down with users and talk about or survey their needs and preferences to make sure your mobility strategy will give them what they really want.

As you work to deliver a superior user experience, look for ways to give people more than they expect and provide useful capabilities they might not have thought of yet. For example:

- Allow people to access their apps and data on any device they use, complete with their personalized settings, so they can get to work right away.
- Empower people with self-service provisioning for any app they need—hosted, mobile or SaaS—through an enterprise app store with single sign-on.
- Provide shared thin clients or other enterprise-grade devices that people can switch to easily when they find that certain apps have been greyed out on their consumer-grade device due to security requirements.
- Automate controls on data sharing and management, such as the ability to copy data between applications, so people don't have to remember specific policies.
- Define allowed device functionality on an app-by-app basis, so people can still use functions such as printing, camera and local data storage on some of their apps even if IT needs to turn them off for other apps.
- Make it simple for people to share and sync files from any device, and to share files with external parties simply by sending a link.

By developing your mobility strategy in a spirit of collaboration with users, you can better meet their needs while gaining a valuable opportunity to set expectations and make sure people understand IT's own requirements to ensure compliance, such as the need to secure apps and data, control network access and appropriately manage devices.

3. Avoid the quadruple bypass

The quadruple bypass represents the worst-case scenario for enterprise mobility: a BYOD user on a consumer-grade device using sensitive enterprise data and going directly to the cloud. This approach completely bypasses the control and visibility of IT—and it's alarmingly common in today's organizations. There are good reasons for this, of course. Cloud apps can help people save time and get their work done more easily, and they can also drive value for the business. The problem comes when cloud apps are used in the wrong way with the organization's sensitive data, compromising security and compliance.

IT policies and user education can only go so far to prevent the quadruple bypass—realistically, if it's the best solution for someone's needs and it seems unlikely that IT will find out, it's going to happen. That makes it essential to provide people with an incentive to work with IT and use its infrastructure, especially when it comes to sensitive data and apps. The best incentive is a superior user experience, delivered proactively and designed to meet peoples' needs better than the unmanaged alternative.

4. Pay attention to your service delivery strategy

Mobile users rely on a variety of application types—not just custom mobile apps, but also third-party native mobile apps, mobilized Windows apps and SaaS solutions. In developing your mobility strategy, you should think about the mix of apps used by the people and groups in your organization, and how they should be accessed on mobile devices.

There are four ways for people to access apps on mobile devices:

Native device experience – In this scenario, the user's device is completely unmanaged. People purchase their own apps, can co-mingle enterprise and personal data freely, and can work over any network. Like the quadruple bypass described above, this is a risky and non-secure approach that should never be allowed for sensitive data.

Virtualized access experience – Virtual apps and data, and virtual desktops as well if desired, are hosted in the datacenter and presented through a remote display protocol. IT can manage access and ensure full security while making it possible for people to run Windows applications on mobile platforms. No data ever leaves the datacenter, alleviating the need for data protection on the device itself. This method does rely on connectivity, which limits offline usage scenarios.

Containerized experience – The organization creates a container on the device where all enterprise mobile apps—including custom and third-party native mobile apps—will be kept separate from other content. IT can manage the apps and data that go into the container while allowing users to provision their own apps from an enterprise storefront. Apps can be updated, provisioned and modified automatically based on IT policies. Network settings such as SSL, encryption and app-specific VPNs can also be included in the container to make it simple for people to connect the right way in any setting. The container can be wiped remotely in the event of loss, theft, device upgrade or employee departure.

Fully managed enterprise experience – This approach maintains complete control over the mobile device with embedded policies for remote wipe, geographic restrictions, data expiry and other security measures. All mobile apps are explicitly chosen and provisioned by IT with no capability for personalization. While this approach is highly secure and suitable for some organizations and use cases, it comes at the cost of a restrictive user experience and isn't compatible with BYOD.

For most organizations, a combination of virtualized access and a containerized experience will support the full range of apps and use cases people rely on. This also makes it possible for IT to maintain visibility and control while providing a superior user experience. People can access hosted applications and native mobile apps—as well as SaaS apps such as Salesforce and NetSuite—through a unified enterprise single sign-on. When an employee leaves the organization, IT can immediately disable the person's account to remove access to all native mobile, hosted and SaaS apps used on the device.

5. Automate desired outcomes

Automation not only simplifies life for IT—it also helps you deliver a better experience. Think about the difference automation can make for addressing common mobility needs like these:

- An employee replaces a lost device or upgrades to a new one. With the click of a single URL, all of the individual's business apps and work information are available on the new device, fully configured and personalized, and ready for work. A new employee or contractor can be onboarded just as easily, with all enterprise mobile apps provisioned into a container on any personally owned or enterprise device. Single sign-on (SSO) enables seamless access to hosted and SaaS applications.
- As an employee moves from location to location and network to network, situational and adaptive access controls reconfigure apps automatically to ensure appropriate security—with complete transparency for the user.
- A board member arrives for a meeting, tablet in hand. All the documents for the meeting are automatically loaded onto the device, configured selectively by IT for read-only access, and restricted to a containerized app as needed. Especially sensitive documents can be set to disappear automatically from the device as soon as the member leaves the room.

- As employees change roles in the organization, the relevant apps for their current position are made available automatically, while apps that are no longer needed disappear. Third-party SaaS licenses are instantly reclaimed for reassignment.

One way to perform this type of automation is through Active Directory. First, link a specific role with a corresponding container. Anyone defined in that role will automatically inherit the container and all the apps, data, settings and privileges associated with it. On the device itself, you can use MDM to centrally set up WiFi PINs and passwords, user certificates, two-factor authentication and other elements as needed to support these automated processes.

6. Define networking explicitly

Different applications and use cases can have different networking requirements, from an intranet or Microsoft SharePoint site, to an external partner's portal, to a sensitive app requiring mutual SSL authentication. Enforcing the highest security settings at the device level degrades the user experience unnecessarily; on the other hand, requiring people to apply different settings for each app can be even more tiresome for them.

By locking down networks to specific containers or apps, with separate settings defined for each, you can make networking specific to each app without requiring extra steps from the user. People can just click on an app and get to work, while tasks such as signing in, accepting certificates or opening an app-specific VPN launch automatically by policy in the background.

7. Protect sensitive data above all else

In many organizations, IT doesn't know where the most sensitive data resides, and so must treat all data with the same top level of protection—an inefficient and costly approach. Mobility provides an opportunity for you to protect data more selectively based on a classification model that meets your unique business and security needs.

Many companies use a relatively simple model that classifies data into three categories—public, confidential and restricted—and also take into account the device and platform used while other organizations have a much more complex classification model and also take into account many more factors such as user role and location. One way to implement a simple model is as follows:

Public data that does not include confidential, privacy or compliance implications can have unlimited data mobility and unrestricted usage anywhere, on any device. There's no need for people to work through the enterprise infrastructure—you can configure app-specific network settings to allow people to connect however it's most convenient.

Confidential data that isn't meant to be public, but poses some minimal risk in the event of leakage, calls for a higher level of protection. In this case, you can provide virtualized access via the enterprise network on BYOD or consumer-grade devices, while allowing full data mobility only on enterprise-grade devices with MDM features such as encryption and remote wipe, or on mission-grade devices designed specifically to protect data in hostile situations.

Some companies may decide that a container-based approach is sufficient for this type of data. In this case, data can be fully mobilized on any mobile device as long as it is stored only within a separate container that can be secured and controlled by IT.

Restricted data posing a significant risk of non-compliance, reputational damage, lost business and other material impact should receive most of your attention. Full data mobility should be limited to mission-grade devices, with virtualized access allowed on enterprise-grade devices. BYOD and other consumer-grade devices should not be granted access at all, or carefully reviewed and considered for virtualization and container-based approaches in certain circumstances.

The model above takes into account both data classification and device type. You may also want to layer additional considerations such as device platform, location and user role into your security policy. Some companies and many government organizations create a larger set of more specific categories of data, each with its own rules.

By configuring network access through your enterprise infrastructure for confidential and restricted data, you can capture complete information on how people are using information to assess the effectiveness of your data sensitivity model and mobile control policy.

8. Be clear about roles and ownership

Who in your organization will own enterprise mobility? In most companies, mobility continues to be addressed through an ad hoc approach, often by a committee overseeing IT functions from infrastructure and networking to apps. Given the strategic role of mobility in the business, and the complex matrix of user and IT requirements to be addressed, it's crucial to clearly define the organizational structure, roles and processes around mobility. People should understand who is responsible for mobility and how they will manage it holistically across different IT functions.

Ownership needs to be equally clear when it comes to mobile devices themselves—especially in organizations where mobility and BYOD go hand-in-hand. Your BYOD policy should address the grey area between fully managed, corporate-owned devices and user-owned devices strictly for personal use—for example:

- Who is responsible for backups for a BYO device? Who provides support and maintenance for the device, and how is it paid for?
- How will discovery be handled if a subpoena seeks data or logs from a personally owned device?
- What are the privacy implications for personal content when someone uses the same device for work?

Both users and IT should understand their roles and responsibilities to avoid misunderstandings. Define your BYOD program explicitly and have participants sign off before they begin using personal devices for work.

9. Build compliance into your solutions

Globally, organizations face more than 300 security and privacy-related standards, regulations and laws, with more than 3,500 specific controls. It's not enough merely to meet these requirements—you've also got to be able to document your compliance and allow full auditability. And that's not to mention your own internal corporate policies. You may already have solved the compliance challenge within your network. The last thing you want to do is let enterprise mobility create a vast new problem to solve. Make sure your mobile devices and platforms support seamless compliance with government mandates, industry standards and corporate security policies, from policy- and classification-based access control to secure data storage. Your solution should provide complete logging and reporting to help you respond to audits quickly, efficiently—and successfully.

10. Prepare for the Internet of Things

Don't just write your policies for today—keep in mind what enterprise mobility will look like in the next few years. Wearable technologies like Google Glass and smart watches will continue to change the way people use mobile technologies, providing a more human, intuitive experience while enabling new use cases. Connected vehicles—including driverless cars—will use data and cloud services in new ways to help people get where they're going more easily and efficiently. Industrial control systems (ICS) will use and exchange enterprise data as part of human workflows as well as behind the scenes. Developments like this will continue to expand the potential of mobility, but they'll also introduce new implications for security, compliance, manageability and user experience.

Pay attention to ongoing industry discussions about emerging technologies like these and design your mobility strategy around core principles that can apply to any type of mobile device and use case. This way, you can minimize the frequent policy changes and iterations that can confuse and frustrate people.

The Citrix solution for secure enterprise mobility

As the leader in mobile workstyles, Citrix provides a complete solution to enable secure enterprise mobility with the simple, convenient user experience your workforce demands. Incorporating complete technologies for MDM, MAM, containerization, application and desktop virtualization, the solution allows ample flexibility to support secure mobility in the right way for each type of information, use case and role in your organization.

The Citrix solution for secure enterprise mobility includes the following products:

XenMobile – XenMobile provides complete MDM and MAM capabilities for secure enterprise mobility management. IT can provide single-click access to mobile, web, data center and Windows apps from a unified app store, including integrated productivity apps with a great user experience. XenMobile also provides business-grade secure email, browser and calendar apps to avoid the security gaps that can be introduced by consumer-grade apps. IT gains identity-based provisioning and control of apps, data and devices, automatic

account de-provisioning for terminated users and selective wipe of lost devices. Integrated Citrix MDX app container technology enables data encryption, password authentication, secure lock and wipe, inter-app policies and micro VPNs to mobile apps.

XenDesktop and XenApp – XenDesktop and XenApp let IT transform Windows apps and complete Windows desktops into on-demand services available on any device. Because apps and data are managed within the datacenter, IT maintains centralized data protection, compliance, access control and user administration on both personally-owned devices and corporate-owned endpoints within the same unified environment. XenApp also makes it simple to mobilize Windows applications for use on smartphones and tablets, and to tweak their interfaces to act like native mobile apps on a mobile device for an optimized user experience.

ShareFile – ShareFile lets you deliver a secure, robust data sync and sharing service that meets all of the workforce's mobility and collaboration needs. A rich, consumer-style experience makes it simple for people to store and sync data across all their devices from any network location. IT can maintain a high level of management and control over file and data sharing, with absolute flexibility to choose where data will be stored, robust device security policies, comprehensive auditing features and integration with Microsoft Active Directory.

NetScaler – NetScaler is an all-in-one app delivery controller to secure, control and optimize the delivery of apps, desktops and services on any device. Broad mobile OS support includes full SSL VPN access for leading mobile OS and handset vendors, including Apple, Google and Microsoft. Micro SSL VPN support lets you define specific connection settings for individual apps without requiring extra steps from the user. Access control, auditing and reporting support compliance and data protection. End-to-end visibility and control gives you greater orchestration of your entire infrastructure and enables effective load distribution across multiple Citrix mobility components.

Conclusion

Enterprise mobility has quickly evolved beyond specific groups and use cases to become a foundational element of enterprise IT. As you develop your enterprise mobility strategy, make sure you're considering the full range of requirements for both users and IT. People expect seamless, convenient access to their data and apps on any device they use, with a user experience that's even better than they're used to in their personal lives. IT needs to be able to provide the right level of control, protection and compliance for each type of data without placing undue restrictions on the ways people choose to work. Citrix solutions offer the comprehensive capabilities you need to support your enterprise mobility strategy, including XenMobile for MDM, MAM and containerization; XenDesktop and XenApp for virtualization; ShareFile for secure data sync and sharing; and NetScaler to secure, control and optimize service delivery to mobile devices. By making effective use of the available models and technologies for security and application and data access on mobile devices, you can deliver the comprehensive mobility strategy your organization needs today and in the years to come.

Additional resources

Case study: How 4 Citrix customers solved the enterprise mobility challenge

Delivering enterprise information securely on Android and Apple iOS devices

The 10 must haves for secure enterprise mobility

Enterprise mobility management: Embracing BYOD through secure app and data delivery

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China

About Citrix
Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud infrastructure to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.