The 10 “must-haves” for secure enterprise mobility

A security framework and evaluators’ checklist

CITRIX®

citrix.com

Becoming a mobile enterprise means new opportunities for your organization. Employees are happier and more productive when they have mobile access to their email, apps and data on tablets and smartphones. Companies running their businesses on mobile workstyle solutions gain competitive advantages and drive top-line growth.

In a recent survey, Aberdeen found that best in class enterprises are three times as likely as all others to tie business workflow to users' mobile devices.[1] Yet, according to nearly every analyst study, security is the primary inhibitor to both enterprise mobility and bring-your-own-device (BYOD) programs. CSO Magazine recently reported that 17 percent of enterprises have already experienced a mobile breach.[2]

Mobile security concerns

While mobile security concerns range from passcode enforcement to device encryption, data breach and data leakage are at the top of the list for implementers of mobile workstyle programs. According to enterprise security expert Jack Gold, organizations will lose three to four times as many smartphones as notebooks each year. Gold (rhetorically) asks us "with 32 or 64 GB of memory, how many records does a lost smartphone or tablet contain?"[3] At an estimated cost of more than $250 per lost record,[4] a data breach can be expensive. In fact, some research estimates the cost of a mobile breach at more than $400,000 for an enterprise and more than $100,000 for a small business,[5] and in some cases these costs can range into the millions.[6] This concern resonates as an increasing number of smartphones and tablets not only connect to the corporate network but also access an increasing number of business applications and content repositories.

Beyond data, enterprise IT and security departments are concerned about the risk of opening up the internal network to a diverse array of mobile devices. In many cases, smartphones and tablets are neither governed nor monitored, meaning that they can introduce network threats and negatively impact an organization's compliance status. There are three primary factors that contribute to enterprises' security concerns.

1. Mobile device and app explosion

With the Center for Telecom Environment Management Standards reporting that 78 percent of organizations allow employee-owned mobile devices in the business environment[7] and enterprise IT spending for Apple® iPad® tablets alone set to reach $16 billion in 2013,[8] mobile devices in the enterprise are not only skyrocketing in volume but are also expanding beyond the executive suites to rank and file employees. Further, whether mobile devices are corporate-issued or personally owned, the number of apps on those devices is increasing. Mobile analysis firm, Asymco reported an average of 60 apps per iOS® device.[9] Given that over half of organizations are supporting more than one device type,[10] the exposure of the corporate network to potentially non-compliant or malicious apps is immense. Though these facts point to a malware risk, consider the *Wall Street Journal* finding in the article, "Your Apps are Watching You": Of 101 mobile apps studied, 56 transmitted the device ID, 47 transmitted location data and five transmitted personal information from the device to a third-party server.[11] Even though the study focused on consumer apps, it points to the fact that devices and the corporate network are vulnerable to the apps that are installed on devices. Even if they aren't considered malicious, apps can access, collect and transmit sensitive data against corporate policy and in ways that can bypass traditional enterprise security monitoring mechanisms.

2. Increasing levels of mobile access

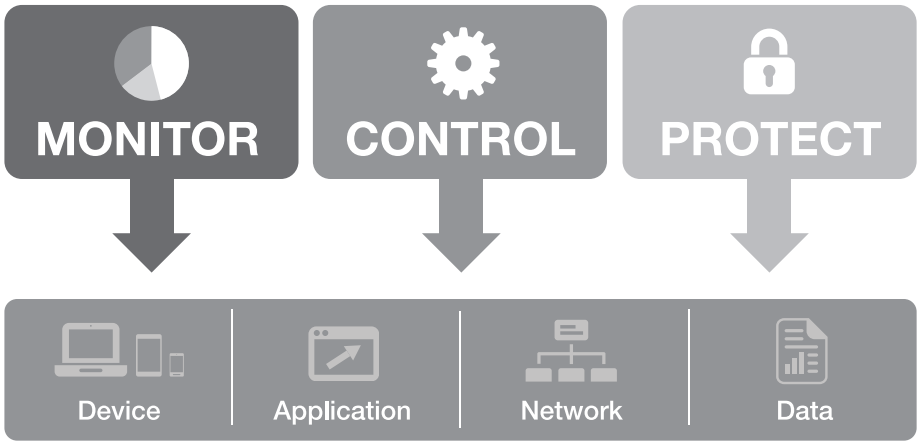
People at all levels of the organization have a strong desire to arm the workforce with mobile devices and mobile access to corporate apps and data. Organizations are also mobilizing horizontally, across their lines of business. According to a Citrix® survey, more than three-quarters of organizations will deploy mobile apps for line-of-business use in 2013, and over half of those will be mission critical. Moreover, 80 percent of organizations are developing custom apps.[12] This can range from restaurant chains equipping hosts and kitchen staff with iPad tablets to airlines distributing the "flight bag" of electronic aircraft manuals, flight plans and compliance documents to its aircrews on their Samsung Galaxy Tabs. Such mobile access shows tremendous promise, but it also means that corporate data and network access will be in the hands of a larger number of users via an increasing number of devices, thus multiplying the risk.

3. Proliferation of consumer-style file-sharing tools

While the security solution for enterprise mobility that we hear about most often centers on locking or wiping a lost or stolen device, the biggest threat is uncontrolled data sharing. With millions of users sharing data across an endless tapestry of cloud-connected endpoints, the potential for data leakage dwarfs that of the device loss/theft scenario. Consumer-style file sharing tools are particularly worrisome because of the multiplier effect: data saved outside the corporate network isn't just shared with one device, but with all of the devices that are connected in a viral manner via the tool. According to the "Citrix Mobile Device Management Cloud Report," some of the most commonly deployed apps, such as Dropbox and Evernote, are also among the most frequently blacklisted by companies, which speaks to their simultaneous usefulness and business risk.[13]

An end-to-end mobile security framework

IT security professionals are largely turning to mobile device management (MDM) or enterprise mobility management (EMM) solutions. However, the range of mobile challenges listed previously requires a new, more-comprehensive security framework – one that goes beyond the basic lock-and-wipe capabilities found in MDM solutions. Today's organizations need a solution that provides them with tools to proactively monitor, control and protect the enterprise from end to end – across devices, apps, data and the network.



The 10 "must-haves" for enterprise mobility

Below are the ten questions enterprises must ask any enterprise mobility vendor.

	Question	Rationale
1	Can I manage any BYO or corporate device?	Many enterprises require foundational device management. They need to centrally configure device security elements such as passcodes and encryption and detect and block non-compliant devices, such as ones that are jailbroken or have blacklisted apps installed. They require the ability to decommission devices when they're lost or stolen, or when a user leaves the organization. Because an increasing number of organizations have both user-owned (BYO) and corporate-issued devices in their environment, the solution should let IT designate ownership easily and set policies and practices accordingly.
2	Can I secure and manage any mobile or web app?	Apps are diverse and don't share common security frameworks. IT needs to centrally secure any mobile or web app or intranet by applying access policies, secure connectivity and data controls to them during or even after the development process.
3	Can I give my users secure alternatives to their killer productivity apps without sacrificing user experience?	What about the killer productivity apps that mobile users need to get their jobs done – email, web, and data access? Users' default position is to use the native app or the app they're used to. But what if enterprises could provide users with a sandboxed, yet stunning, alternative to the native email client, browser and file-sharing tools they know and love?
4	Can I offer secure mobility and protect user privacy?	While many organizations choose to solve their mobile challenges with a full-stack enterprise mobility management solution, organizations subject to stringent user privacy rules may opt for a lighter-weight approach. This could mean deploying only an email client or secured app to the device. The solution should be flexible enough to enable either scenario or a mix, say for a global enterprise that wants to manage devices for its U.S. employees but only provide a sandboxed email client for its German personnel.
5	Can I give my users SSO and make any app available on any device?	Single sign-on (SSO) is one of the few security features that provides something for everyone. IT can provision and de-provision apps more easily and ensure mobile app access for terminated employees is de-activated immediately. Users get simple access without having to authenticate on a small screen. This is a must-have for any mobile enterprise. If the enterprise is truly going mobile, chances are IT will need to provision not just mobile apps, but web, SaaS, Windows, and data center apps as well. IT needs to make them available all in one place: a unified app store.
6	Can I provide scenario-based network access?	With the array of mobile devices accessing the network, IT needs to define comprehensive access and control policies using endpoint analysis and user roles to determine which apps and data to deliver, and what level of content access to provide.
7	Can I let my users access their content while still protecting data?	Mobile users need access to corporate content, but there is a dearth of tools that allow IT to manage this access and control data. Whether content resides in Microsoft® SharePoint® or in a data sharing & sync app, IT should be able to set and enforce data policies that dictate what users can and can't do with the content – save, email, copy/paste and so on.
8	Can I be flexible, providing the right security for the situation?	Similar to the challenge of balancing security and privacy is the need to apply the right security for the situation. IT needs flexible solutions that support a "good-better-best" approach to security, making the right tradeoffs between security and usability.

9	Can I integrate mobile with existing IT resources?	IT understands the security hazards of technology silos. Enterprise mobility solutions should easily "snap" into the existing IT environment. This means direct integration with enterprise directories, public key infrastructure, corporate email, access technologies such as WiFi and VPN and virtual desktops and apps. It also means integration with Security Information and Event Management solutions and log management systems so IT can report on mobile alongside other infrastructure.
10	Is your architecture secure, scalable, and highly available?	Enterprise mobility management solutions must be enterprise-grade. This means that they are architected to keep sensitive user data behind the firewall, not exposed to the Internet. It means that organizations can grow their deployments without increasing complexity. It also means that industry-standard high availability configurations ensure system failover and straightforward failback should the technology fail.

End-to-end mobile security

Organizations pursuing enterprise-grade mobility need to look beyond MDM and consider mobile security in an end-to-end way – across devices, apps, the network, and data.

Mobile device security challenges and requirements

Centralized management of device security

I need to configure devices and enforce policy. Many enterprises need to configure device security components such as passcodes and encryption, as well as enforce policy, in a centralized manner. As mobile workstyles move into the mainstream, the increasing number of devices and users accessing the network from more than one device is generating an urgent need to centrally manage those devices and enforce role-based security policies. When devices are lost or stolen or users leave, those devices need to be centrally locked or wiped of corporate data for security and compliance purposes.

Fragmentation of mobile device platforms

Help! No two devices are the same! Employees demand device choice, and for many organizations, it's an attractive strategy. It may help them attract and retain talent or save on device costs. But unlike standard-issue, locked-down PCs or tightly controlled BlackBerry® handhelds, mobile devices in today's enterprise are diverse, have varying levels of vulnerability and offer no consistent way for IT to manage even the most basic security policies. According to Aberdeen Research, the average best-in-class company supports 3.3 mobile platforms,[14] including iOS, Android®, Windows® and BlackBerry. Fragmentation presents unique security challenges from an IT standpoint, including how to monitor, provision, support and secure multiple apps across the different platforms, or ensure that employees have installed the proper OS security patches and updates.

BYO vs. company-issued devices

I have a BYOD program and now I'm rolling out a corporate iPad initiative. Organizations are increasingly managing BYO devices alongside corporate-issued devices. They need to designate ownership in a way that's accurate and compliant, manage each type according to its policies and processes and report on them on an ongoing basis.

Mobile device security requirements

According to the above security framework, below is a set of device-oriented requirements for enterprise mobility solutions.

Monitor	Control	Protect
• Audit and report on devices by ownership type – BYO or corporate issued • Report on device details (type, OS, version, device integrity, etc.) • Inventory installed apps • Ascertain device usage (e.g., the device is roaming) • View device location (and take action if a user has removed the device from a pre-defined geo-fence) • Determine a device's compliance status (e.g., jailbroken, blacklisted app)	• Deploy policies in a similar manner across diverse device platforms and OSs • Push corporate security and regulatory compliance policies (e.g., passwords) to every device • Audit devices at pre-configured intervals to ensure that no IT-mandated policies have been disabled • Block network access for any device that is out of compliance • Set security policies to prevent employees from accessing device resources or apps	• Enable user self-service for lost or stolen devices • Locate, lock and wipe devices upon loss or theft • Wipe or selectively wipe devices once users leave the organization

Mobile app security challenges and requirements

Any app on any device

I need to keep track of and manage all the apps that users want mobilized. Users love their apps and want to use them to get their jobs done. Lines of business are developing apps for their workers. But IT needs to manage it all – centrally provision mobile, web, SaaS, Windows and datacenter apps and make it easy for users to get them from one place.

Centralized, consistent app security

How do I maintain any level of consistent security in this app free-for-all? With thousands of mobile apps to deal with, IT is in a losing battle to secure apps and intranets in a centralized and consistent way. Organizations must contend with an array of custom and third-party apps, none of which uses a common development framework, has common security features, has the same authentication methodology or accesses data in the same way. Yet IT needs to apply a set of common policies to each of those apps!

Security of killer productivity apps

What my users really want is their email, web and docs. Most users need a core set of killer or "must have", mobile apps – typically email, web and data access. IT needs to make sure those apps are secure, but today they're not. IT can no longer deal with potential data leakage from email, unsecured access to intranets or a user uploading the corporation's confidential financials to a consumer-style file-sharing tool. However, users have come to expect a fantastic native experience and have little tolerance for anything less. What's needed is a set of acceptable secure alternatives to the killer apps.

Protection of user privacy

It's not just about enterprise security, but my users' privacy too. Full-stack enterprise mobility management solutions come with core features such as the ability to GPS-locate a device or view installed apps on users' devices. Even though those capabilities can be disabled in many solutions, some organizations may not even want the appearance of privacy infringement. Organizations with heightened user privacy concerns or subject to privacy regulations need a way to provide enterprise access to mobile users without managing the whole device. For example, an organization may wish to provision only a sandboxed email client to users so they can access corporate email, but not require wholesale device management.

Federated identity and SSO

Make access simple for me…and for my users. Organizations pursuing mobile workstyle projects are providing a multitude of apps to users. Given the diversity of apps and app types, it's difficult for IT to provision access in a role-based way. What's more, it's even more difficult to keep track of all the apps that IT needs to de-provision once a user departs the organization. This is especially true of SaaS apps, which often get forgotten because the user credentials may be managed separately and the app may be out of IT's line of sight. On the user side, it's hard to log into these apps individually each time access is needed. With two apps, it's not a problem. With five, it's really tedious. With 10, you've got users rioting in the streets.

Mobile app security requirements

According to our security framework, below is a set of app-oriented requirements for enterprise mobility solutions.

Monitor	Control	Protect
• Get an inventory of mobile apps installed on devices • Ensure – and report for compliance purposes – that users' app access privileges are fully revoked when they depart the organization	• Make any app – mobile, web, SaaS, Windows, or datacenter – available to any device via an unified app store • Secure custom or third-party apps centrally, and apply granular policy controls during or after development • Provide stunning, yet sandboxed alternatives to killer productivity apps • Control user access to apps with SSO across all app types	• Provide secure app and intranet connectivity without a full-bore VPN • Protect sensitive corporate data with consistent in-app data controls • Prevent users from accessing apps and data after they depart the organization • Protect user privacy by enabling access to corporate email, intranets or apps without managing the whole device

Mobile network security challenges and requirements

Inability to control access

I've got some mobile users in the office with compliant devices, some with jailbroken devices and some on unknown devices at Starbucks. When it comes to access, one size doesn't fit all. With the array of mobile devices accessing the network, IT needs a way to define comprehensive access and control policies using endpoint analysis and user roles to determine which apps and data to deliver and what level of content access to provide.

Inability to meet mobile network demands

I'm not sure my mobile network can handle the usage, especially during peak periods. While not directly related to security, a key consideration that touches mobile security is scalability of the mobile network. As more enterprise users access the network via an increasing number of devices and organizations deploy an increasing number of critical mobile apps, IT needs to scale to accommodate increasing volumes of mobile traffic and deliver mobile apps with high performance.

Mobile network security requirements

According to our security framework, below is a set of network-oriented requirements for enterprise mobility solutions.

Monitor	Control	Protect
• Analyze mobile endpoints for compliance status	• Control network access based on device configurations, device status, user role and other factors such as which network a user is on • Meet mobile network demands, including load balancing mobile requests and ensuring high-performance mobile app delivery	• Protect the corporate network from mobile threats such as malware

Mobile data security challenges and requirements

The Dropbox problem

I have a Dropbox problem. Consumer-style file-sharing tools have become popular in enterprises because they are easy to use and solve a real problem: how to get access to the latest data from any device. While useful, these apps also pose a large data leakage risk. Organizations can't monitor or protect data in these apps, and while they could blacklist the apps themselves, that approach doesn't solve the problem for users. Organizations need a secure alternative to these tools that solves users' problems while allowing IT to encrypt data and control access and usage through granular data policies.

Containers create data silos

Sandboxed apps make it difficult for my users to get to the content they need. App or data containers – the enterprise mobility industry's response to data leakage to date – pose daunting challenges for usability. Very often, users can't access the documents they need in the app they want, and they can't share content across apps. This makes content review, editing and collaboration cumbersome or impossible.

Monitor	Control	Protect
• Track and alert on mobile user access to data	• Provide "follow-me data" for mobile • Enable mobile users to securely sync and share data to and from mobile devices • Set granular data control policies • Share data controls and allow access across apps	• Protect mobile data by encrypting it at rest and in transit • Prevent data leakage with a secure, encrypted data container • Protect data by wiping the container upon user departure or device loss, or based on other events such as device jailbreak

Additional security considerations and requirements

The right security for the situation

I have full-time employees and contractors. They don't all need the same level of security. Similar to the user privacy example, IT needs the flexibility to apply appropriate security measures to the situation at hand. Organizations have diverse users. Some are knowledge workers using a corporate-issued device for work and personal activities. Some are shift workers who share a device with other workers. Still others are contractors who have brought their own device. Mobile security cannot be one-size-fits-all. In the situation above, IT may need to be flexible, providing full-stack mobile enterprise access and security to the knowledge workers, while only managing the shared devices and provisioning one or two work-specific apps but no email, and provisioning only an email client to the contractors.

IT also needs the flexibility to take a good-better-best approach to security based on the risk profile of the organization. Using email as an example, a highly regulated organization may choose a completely sandboxed email client with tight data controls. A less-regulated but still security-conscious organization may opt for a native email experience but still encrypt email attachments. An unregulated organization may deploy native email and simply wipe corporate email in the event of device loss or theft or employee departure.

Enterprise integration

Don't give me another silo to manage. IT understands the security hazards of technology silos. Enterprise mobility solutions that aren't directly integrated with the rest of IT creates both management and security challenges. For example, mobility solutions that don't integrate directly with LDAP, but instead cache user data on a periodic basis, pose the risk that terminated employees may be able to access enterprise apps and data from their mobile devices during the period between when they're let go and the next time the solution synchronizes directory data. Similarly, mobility solutions that don't integrate with SIEM and log management tools prevent IT from having a complete security or compliance picture.

Enterprise-grade architecture

What good are security features if my CEO's personal data is exposed to the Internet? Many enterprise mobility solutions are not architected with security in mind. Rather than keeping sensitive data behind the firewall and broker access to it via a proxy in the DMZ, they cache user data temporarily in the DMZ where it is exposed to the Internet. Additionally, many solutions do not scale to meet the demands of growing mobile populations. Some solutions require IT to manage multiple instances of the same solution in separate silos. Similarly, high availability is a necessary feature IT professionals expect, though few solutions provide it fully. Some solutions don't have built-in redundancy with industry-standard clustering for failover and straightforward failback. As mobile workstyles become mainstream and apps become increasingly mission-critical, enterprise readiness of mobile solutions is increasingly important to IT.

Additional requirements

Below are additional security requirements for enterprise mobility solutions.

Monitor	Control	Protect
• Integrate mobile data with SIEM and log management tools for better security visibility and compliance reporting	• Deploy the right level of security for the situation (e.g., email to users in highly regulated industries, app security without device management to contractors) • Control access at all times with direct integration with enterprise directories • Control access and enable SSO with PKI integration • Provide access to email with enterprise email integration • Control enterprise access with direct integration with VPN and WiFi solutions	• Protect privacy by keeping user data behind the firewall • Protect mobile users from downtime with industry-standard high availability • Future-proof the mobile enterprise by deploying a scalable solution that accommodates mobile device growth without increased complexity

Conclusion

While enterprise mobility brings opportunity for your users and organization, it also invites risk. Organizations can use this white paper as a mobile security framework and a checklist for evaluating enterprise mobility vendors.

About Citrix XenMobile

Citrix XenMobile is an enterprise mobility management solution that enables complete and secure mobile device, app and data freedom. Employees gain quick, single-click access to all their mobile, web, datacenter and Windows apps from a unified app store, including beautiful productivity apps that seamlessly integrate to offer a great user experience. The solution provides identity-based provisioning and control for all apps, data and devices, policy-based controls, such as restriction of application access to authorized users, automatic account de-provisioning for terminated employees and selective wipe of apps and data stored on lost, stolen or out-of-compliance devices. With XenMobile, IT can meet users' desire for device choice while preventing data leakage and protecting the internal network from mobile threats.

1. "Mobility in ERP 2011", Kevin Prouty, Aberdeen, May 2011
2. "Global State of Information Security Survey", CSO Magazine, 2012
3. "MDM is No Longer Enough", Citrix webinar with enterprise security expert, Jack Gold, October 2011
4. "U.S. Cost of a Data Breach", Ponemon Institute, March 2011
5. State of Mobility Survey, Symantec, February 2012
6. In 2010 the average cost of a data breach was $7.2 million. Doug Drinkwater, Feb. 10, 2012, TABTIMES.COM
7. marketwatch.com/story/ctemsr-research-78-of-enterprises-allow-bring-your-own-device-byod-2012-07-24?siteid=nbkh
8. "Global Tech Market Outlook for 2012 and 2013" Andrew Bartels, Forrester, January 6, 2012
9. "More Than 60 Apps Have Been Downloaded for Every iOS Device", Asymco, January 16, 2011
10. "Market Overview: On-Premises Mobile Device Management Solutions", Forrester, January 3, 2012
11. "Your Apps are Watching You", *The Wall Street Journal*, section, December 17, 2010
12. 'Mobile Gets a Promotion' infographic, Citrix, October 2012
13. Citrix Mobile Device Management Cloud Report, Q3 2012
14. "The Need for Mobility Management", Aberdeen blog, February 2010

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 the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.