7 MUST HAVES FOR MOBILE APP SECURITY

Overview

Mobile devices are not just another type of endpoint. Inherent features (e.g., camera, accelerometer, proximity sensor, etc.) coupled with the always-connected, readily available nature of these devices represent an opportunity for improvement in enterprise user productivity.

Enterprises can begin to realize this potential by allowing use of corporate data in both custom-built and commercially available mobile apps. Mobile workflows resulting from interactions between these apps can be faster and more intuitive than those on a PC. However, the need to always retain control over corporate data should give an enterprise pause before sanctioning the widespread use of sensitive business information on mobile devices.

Having to trade usability against security puts enterprises in an unenviable position. Below are the minimum requirements that an enterprise must have in a mobile app security solution in order to transform the mobile user experience without compromising on security.

#1 Data Protection on Any Device via Containerization

New advanced app-level controls available in popular mobile OS platforms still require that the device be controlled via Mobile Device Management (MDM). While device management may very well be a key component in an enterprise's mobility strategy, a company may not want to – or have the ability to – enforce its use in all scenarios. Scenarios include personally owned devices, devices used in the extended enterprise (e.g., business partners, distributors, board members, etc.), and devices used in regions with strong user privacy regulations. The heterogeneity of the mobile device landscape, supported by a myriad of mobile operating systems and versions, device form factors, inconsistent device management status and differing ownership models, all contribute to the IT management headache.

What's needed is a mobile security solution with next-gen app containerization that utilizes app-level device-independent encryption to secure corporate data. Such a solution will provide the same advanced protection regardless of device ownership (i.e., BYOD or corporate-liable) and management status (i.e., controlled by MDM software or not).

#2 Consistent Security Across OS Platforms

Mobile OS vendors provide security capabilities that are not common across OS platforms. In the corporate world, where the mobile device landscape is becoming increasingly heterogeneous, the lack of a common security paradigm across OS platforms causes unnecessary IT management overhead.

A mobile app security solution that provides consistent security management across mobile OS platforms reduces IT administrative costs. Additionally, with the majority of mobile users having multiple devices, providing a familiar security experience across platforms and form factors allows users to continue working they way that they are used to, without impacting the productivity they derive from their mobile devices.

#3 Authentication To Match Your Security Requirements

Mobile OS platforms, even those with app-level password controls, enable security with one device-level passcode. Ways to bypass this passcode continue to make the news. Complex passcodes, which provide greater protection, can be enforced on devices under MDM control but that impacts the user experience.

Authentication in a mobile app security solution should be adaptable to address your enterprises security requirements. Apps and their data must be protected with passwords and cryptography that is independent of any underlying device-encryption. For devices under MDM control, this allows enterprises to enforce simple device-level passcodes so as to not impact the user experience. If the device passcode is hacked, the app data will still be encrypted – even if viewed via low-level file system access. When the device is not under MDM control, app-level device independent encryption still ensures protection. A mobile app security solution should also support 2-factor authentication for environments that have more stringent access requirements.

#4 Mobile Business Workflows That Users Want

While important, sharing of documents, photos, movies, etc., between apps just scratches the surface of what becomes possible with mobile devices.

A mobile app security solution should also allow apps to securely share metadata, documents, and even services with each other, providing an efficient, streamlined workflow. For example, one app could call upon a print service that is actually part of another app, sharing both the document to be printed as well as the metadata to ensure the document will be printed on A4 paper, with a half-inch margin, and all the text in boldface. Such an approach allows for a variety of published services to be pulled together into a single app to provide users with desired workflows. A user can accomplish a multitude of different tasks – note creation, printing, emailing, instant messaging, file sharing, and web/URL launching capabilities – without having to manually navigate between one or more apps.

#5 Control Over The Flow of Data

Mobile devices typically contain a mix of corporate apps that will need enterprise management and unmanaged personal apps. A continuing concern for businesses is preventing the breach of sensitive information. For example, credit card data, subject to PCI DSS, could be copied from an enterprise app to a consumer app that stores data unencrypted in the cloud. Additionally, businesses are also concerned about non-corporate information making its way into the enterprise domain, which could expose the corporation up to legal action.

A mobile app security solution should allow a business to determine the flow of data in and out of the enterprise domain. Opening of data from a managed app to another app, managed or not, should be controllable – this can address data leakage via apps that write to the consumer cloud. Copy/paste of corporate information from a managed app to an unmanaged app should be preventable. Data being transferred between two managed apps should always remain encrypted, even when temporarily cached to disk. Opening of data from an unmanaged app to a managed app should also be preventable. This ensures clear segregation between personal and corporate data, critical when a remote wipe of corporate data is needed.

#6 Happy Users

For some mobile OS platforms, MDM controls can be used to toggle whether or not the device can be backed up to default cloud storage. Enterprises might choose to prevent this backup for managed devices because corporate data could then be synced to non-managed devices. Similar MDM controls can control syncing of contacts to the cloud. The downside of enabling these controls is that users of managed devices will not be allowed to backup their personal data or contacts.

In mobile, the user experience is paramount. Security controls that hamper this experience, especially when a device is used for personal tasks, will incent users to find a workaround. That's a potential threat to your data. With a mobile security solution that offers next-gen app containerization, an enterprise can permit backup of the device to default cloud storage. The user experience is preserved as personal apps and data can be backed up as usual. At the same time, corporate security requirements are met as next gen containerization ensures that data in enterprise apps is protected with device-independent encryption and therefore backed up securely.

#7 Supporting the Extended Enterprise

Many enterprises are starting to think beyond the employee productivity improvements that are enabled by mobility. These enterprises are wondering how they can achieve similar benefits across their extended enterprise (e.g., business partners, distributors, board members).

In the extended enterprise, MDM is not a realistic option for corporate data security. MDM leverages a users' group membership in the corporate directory system (e.g., Active Directory) to automate policy and access controls. Adding non-employees to the corporate directory is not something that IT will easily permit. Additionally, there can only be one MDM profile on a device and so device management cannot support cases where a user needs to access sensitive business data from different enterprises – e.g., a director who sits on the board of many companies.

Your mobile app security solution should be flexible enough to enable secure use of sensitive business information in the extended enterprise, while still ensuring that the enterprise has complete control over this information. Mobile app containerization that doesn't require membership in the corporate directory system will enable broader use of corporate data, without adding unnecessary IT administrative overhead or compromising on enterprise security.

Conclusion

Enterprises should not have to compromise on usability in the name of security. Enterprises looking to secure their mobile apps should ensure that these seven must-haves are present in solutions that are being evaluated. If requirements are met, enterprises can help transform the mobile user experience by permitting the widespread use of corporate data in simplified, intuitive, mobile workflows safe in the knowledge that business information is always protected.

About Good Technology

Good Technology is the innovation leader in secure mobility solutions; enabling business to move freely and engage at the edge. Good's comprehensive solution consists of a secure mobility platform, mobile device management, a suite of collaboration applications, and a broad third-party application and partner ecosystem that unlocks your mobile potential. More than 5,000 organizations in 130 countries use Good Technology solutions, including FORTUNE 100™ leaders in commercial banking, insurance, healthcare, retail, government, and aerospace and defense. Learn more at www.good.com.

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

EMEA Headquarters
+44 (0) 20 7845 5300

Asia / Pacific Headquarters
+1 300 BE GOOD