SOPHOS
Security made simple.

Mobile Containers Explained: The Russian Dolls of Mobile Security

Whether a company implements a Bring Your Own Device (BYOD) program or Choose Your Own Device (CYOD) program, the number one concern is the same: security. It doesn't matter who owns the mobile device used to access corporate assets. If it's lost or stolen, corporate data is at risk. Many IT organizations focus on locking down mobile devices to prevent use of the device if it becomes lost or stolen. But the security issue isn't the device itself. It's the data, and that's where containerization comes in. Containers enable you to protect sensitive data and emails on tablets and smartphones regardless of who owns the device. Containers give IT the controls needed to protect corporate data, without impacting users' personal data or their productivity.

Business Security Versus Personal Privacy

Nearly everyone relies on mobile devices not only for work but as an integral part of our day to day lives. They are our social connection to the world. They serve as cameras, calendars, and occasionally we use them to call someone. Nearly all employees purchase their own smartphones and tablets. Everyone wants to be connected and work on the go – be it on the train ride home or in the doctor's waiting room. Access to corporate files and email from a mobile device is the norm, not the exception.

Today there are 2.6 billion smartphone subscriptions globally. By 2020, there will be 6.1 smartphones in circulation globally. **– Ericsson Mobility Report**

Thanks to this proliferation of mobile devices, corporate data no longer resides safely within data centers. It moves on and off the corporate network and across unprotected public networks via hundreds – even thousands – of mobile devices. This information ranges from contact information to sales presentations, from project proposals to spreadsheets. For most users, nothing is off limits when trying to get work done on the go.

4.3% of company-issued smartphones are lost or stolen every year. **– Kensington**

Every document, email or file stored on a mobile device is at risk. Given their small form factor, mobile devices are easily lost, forgotten or stolen. In any of these situations, corporate data can end up in the wrong hands. But an attacker doesn't need physical possession of a mobile device to access the data on it. Data can also be extracted by malware embedded in malicious applications. Users tend to accept application permissions without really considering them and, in doing so, can inadvertently grant malicious applications access to contact and other sensitive data residing on the phone.

Protection from Potentially Unwanted Applications (PUAs) is an afterthought for many. Users just think about the benefits of apps to themselves – whether it's a flashlight app or an app to make dinner reservations – users are rarely bothered by the fact that many apps ask for unnecessary permission to cameras and other sensitive information such as contacts.

Whether the device is personally owned or company supplied, people – especially millennials – use their devices for both work and personal matters. And, to make matters more complicated, they demand privacy. That means organizations can't simply wipe a lost or stolen device if doing so will also delete the user's personal data. In some jurisdictions, an organization can be held liable for an employee's personal data. Even when users have separate personal devices, there is always some personal information on nearly all corporate devices.

Unfortunately for IT, no single mobile device appeals to every user . If IT only had to manage iOS, Windows and Android, that would be one thing. Not only are there significant functional, management and security variances between the 3 OSs but, according to OpenSignal, the fragmentation of the Android market has resulted in more than 24,000 distinct Android devices. Each hardware manufacturer makes modifications to the OS to improve its handsets' capabilities. Google can release a new version of its OS, but it has no control over whether OEMs push it out to their devices. All this fragmentation means that IT organizations have to individually touch each device to show users how to implement the proper security controls.

The Answer: Secure Mobile Containers

The most effective way to address these data security and privacy challenges is to deploy a mobile container. A mobile container creates a separate, secure area on a mobile device in which users can access corporate data and applications. The container is authenticated and encrypted to protect and isolate data from unauthorized access, malware, other applications and system resources. The container is downloaded as software onto the mobile device and, within that container, users can download and run protected applications.

Many mobile device manufacturers provide native containers. However, a third-party mobile container provides both security and consistency across multiple platforms, thereby addressing a key challenge IT organizations face: how to efficiently manage a diverse fleet of mobile devices. A mobile container makes it easy to manage data on mobile devices, whether they are personally owned, company issued, any of the various flavors of Android, Windows and/or iOS.

Let's take a look at the key types of mobile containers:

An **email container** serves as a personal information management (PIM) container solution for email, calendar and contacts, and is the primary use case for many organizations. The container creates a consistent and secure email experience for every user, regardless of the device. Corporate provisioned email, calendar and contacts are isolated from other applications on the device, giving IT the ability to wipe just the corporate assets if an employee leaves the company or the device is lost or stolen. IT also has the option of requiring additional password protection for work email. In addition to protecting email, calendar and contact data, an email container offers the added benefit of solving the Android fragmentation issue.

A **content container** provides a secure workspace with rights management, enabling user productivity and IT control over corporate data. Users can access, collaborate on and share documents. This helps ensure that everyone is working off the same document. IT can control how users alter, share and distribute documents, as well as how and which cloud storage application they can use. Integration with file encryption enables encrypted files to be sent to the content container and opened only if the device is in a secure state and the user can validate his/her identity with a password. Encryption can also be monitored and controlled so that only encrypted files are stored in the cloud.

FACTORS TO CONSIDER WHEN DEPLOYING A MOBILE CONTAINER SOLUTION

- What kind of data do you push out to your employees?
- What files and documents do you want to keep secure?
- What OS do you need to use?
- Do you need to enable email communication across multiple versions of Android?

A **corporate browser** can also be deployed within a container to provide secure browsing access. IT can push the most frequently used business-related and corporate websites to users for secure access. The browser also simplifies single sign-on to corporate intranet sites and other frequently accessed websites. However, IT can enable or disable "save password" functionality to reduce risk for important corporate sites and can prevent the copying of sensitive data outside of the corporate browser.

Mobile containers can be thought of as the Russian Dolls of mobile security where each doll represents a different layer of encryption. The first, largest doll is the encryption of the mobile device. The next doll is the mobile container, which is also encrypted, and the smallest doll is the encrypted file. Thus, containers within containers provide multiple layers of encryption.

Containers: Just One Piece of a Mobile Security Strategy

While mobile containers play the starring role in securing corporate data on mobile devices, other elements must also be incorporated to create a holistic mobile security strategy. For example, anti-malware protection is critical for Android devices, which are at a higher risk of infection than iOS. It is also important for IT to have a means of enforcing security controls such as the use of strong passwords and blocking jailbroken devices. An additional unique password should be required to access the container, but access should only be granted after the device is inspected to ensure that it has not been rooted, jailbroken or infected by malware.

Containers should be easy to use and the encryption seamless for end users. However, that doesn't mean IT organizations can bypass user education. Particularly in the case of BYOD, users must understand why a container is required, what protection it offers, and its implications on usability. For example, users must understand that their device passcode could continue to be a four-digit PIN, but the container itself will have a separate, longer passcode to make it more difficult to crack.

A mobile security strategy should also include a self-service portal that enables IT to offload some help desk tasks to users. For example, with IT's consent, users should be able to enroll their own devices, deploy a container and other corporate applications, reset passcodes, lock and wipe their device, and decommission a device.

The containerization solution should also be integrated with the corporate Wi-Fi network to prevent an unhealthy or compromised device from connecting to corporate resources. If an unhealthy device attempts to connect to the network, the solution should lock down the container, isolate the device and put it in quarantine or, if the device is compromised, prevent it from syncing with the email server.

Finally, encryption is a critical piece of a mobile security strategy. Encryption protects data within the container. File encryption can also be added for an additional layer of security if files need to be shared outside of the company.

Conclusion

Regardless of the type of mobility program an organization chooses to implement – BYOD or CYOD – securing data on mobile devices is a pre-requisite. Mobile containers are the best way to separate personal and business information, enabling organizations to secure against data loss and malware while protecting user privacy. But while containers are a significant part of a mobile security strategy, they are not the only part. Look for a technology provider that can help you create a holistic mobile security strategy that has at its core a robust mobile container. Above all, the provider should make security simple for users and IT alike.

Introducing Sophos Mobile

With Sophos Mobile you can secure your mobile devices without slowing users down. It features powerful container options that keep corporate data secure without locking down the entire device. The straightforward management dashboard makes it easy for IT to setup and maintain devices, and quickly respond to issues. It integrates both with Sophos UTM, enabling admins to block Wi-Fi and VPN access for non-compliant devices, and with Sophos SafeGuard, enabling users to access encrypted data on their phones and tablets.

Sophos Mobile includes email, content and native OS containers, as well as a corporate browser. Highlights include:

- A secure solution for corporate email, calendar and contacts
- Secure access to files on mobile devices with the ability to edit and create
- Control access and publishing rights for cloud storage (e.g. Dropbox, Google Drive)
- Secure browsing access to the most used corporate sites
- Support for native containers - Android enterprise (Android for Work), Samsung Knox, and iOS managed
- Award-winning anti-malware protection, powered by SophosLabs

Try it now for free

Try the online demo or download a free 30-day trial at sophos.com/mobile.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

2017-03-17 WP-NA (MP)