Securing BYOD and Mobile Collaboration

Seclore FileSecure Lite for Mobile balances the trade off between collaboration and security

With Great Technology Comes Great Risks

The benefits of mobile devices and are numerous: from reduced costs, to greater employee satisfaction, to increased productivity. However, every new technology arrives with its own set of challenges. According to Gartner,

- 50% of all organizations will require employees to supply their own device for work purposes by 2017
- Security remains the top concern for BYOD

Despite the proven business benefits of BYOD and Mobility, security remains the top challenge for organizations today. The company does not necessarily own the device but owns the information on it – and this is a new problem that orthodox security solutions are unable to completely solve. Companies have limited control on their employees' personal devices, and technologies such as MDM (Mobile Device Management) are already starting to raise privacy-related eyebrows. Encryption – the most common security measure in use today – is black-and-white at best. When the information is decrypted, all the security is lost. Not to mention the difficulty of deploying a full-fledged encryption solution on a device you do not own.

Traditional perimeter-based security tools fail to secure the information once it leaves a specific boundary or jurisdiction. In today's world of dissolving perimeters, this approach no longer works. Securing just the perimeter or the device where the data resides is no longer feasible. With information being accessed on multiple platforms, devices, and locations - the number of data leakage points has increased drastically. And so has the risk.

Recipients – both inside and outside your enterprise – need easy access to protected information on-the-fly on their own devices, without the need for complicated installs and change management. They want easy access to cloud-based file-sharing services and need to move data across different applications, cloud systems, and geographies – which may include their personal Dropbox account. IT departments need to balance the enterprise's need to work and collaborate productively using the latest technology – without compromising on security.

What you truly need is a solution that secures your information and mitigates your risk regardless of where your sensitive information assets reside – on any device or platform.

[1]Gartner. (2013). Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes

Information-Centric Vs. Device-Centric Security

Information Rights Management (IRM) is a technology that protects information regardless of where it goes and how it is accessed. It encrypts information and then enables information owners to assign granular usage policies to their information. These policies allow information to be accessed and utilized access based on four criteria:

These IRM security policies are persistent; they 'stick' to the information wherever it goes. They are also completely dynamic; you can change access levels (or revoke access) – even after the information is distributed. All activities performed on all protected files are logged against the respective users and a complete audit trail is available.

Files can also be deactivated remotely – thus expiring the information in real-time. Hence, if a mobile device is lost or stolen, the information will remain inaccessible.

Securing the Message, Not the Medium

Seclore FileSecure virtually eliminates the need to secure and control the device on which information is accessed. Since the information itself is secure and controlled, the risk of BYOD and Mobile Collaboration is significantly reduced.

When a file is protected with Seclore FileSecure, the traditional barriers to security break down: there is no 'data in motion', 'data at rest' or 'data in use'. You don't need separate security for each of them. With Seclore FileSecure IRM, data remains protected at all times – in motion, at rest, and in use. The risk of even authorized users misusing the information – while they are using it - is virtually eliminated.

Locking Information to a Particular Device

Information can also be locked to a particular device. With this feature enabled, even authorized users would be unable to access protected information on any device other than the authorized ones.

For example: a user could be allowed to access a file from his office computer, but not his mobile phone or home laptop.

FileSecure Lite for Mobile

FileSecure Lite for Mobile enables secure and safe information exchange and usage on mobile devices. Protected files can be accessed as easily as unprotected information – with no change in user experience. This security is information-centric - and not perimeter-centric or device-centric. This eliminates the need to worry about the security of the device, since the information will always remain safe.

Since mobile operating systems restrict third-part applications from controlling screen capture capabilities, all information is rendered with a watermark - which contains the username, the organizational server name, and the timestamp to reduce the likely-hood of information sharing.

Figure1
Seclore Filesecure Lite in the Appstore

Figure2
Watermark Viewing of Protected Content

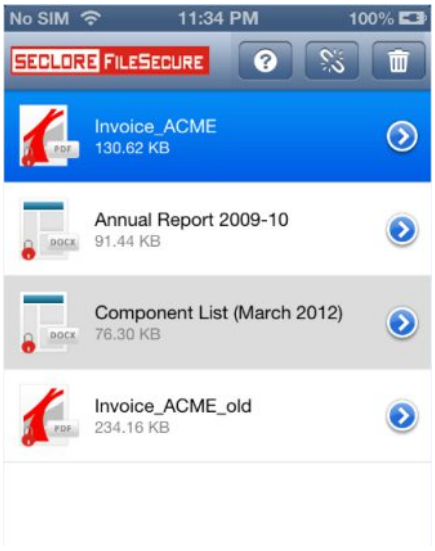

Figure3
List of Previously Viewed Files

Supports both iOS and Android Devices

Available on the App Store

Available on the Android Market