MobileIron
WHITE PAPER

Mobile First: Securing Information Sprawl

January 2014

Contents:

MAKING ENTERPRISE MOBILE FIRST

MobileIron

415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

Introduction: Addressing Information Sprawl – The Next Mobile First Challenge

In a recent survey, “The Mobile Trust Gap,” MobileIron reported that of the 3000 respondents, 80% claimed they are using personal smartphones and tablets for work. In November 2013, 451 Research reported that **41% of enterprises increased spending on Mobile Device Management (MDM) in 2013,** with **46% planning to do so in 2014.** It’s clear; the question is no longer if but rather when and how businesses will bring mobile devices under management. (For a detailed discussion of how to support a multi-OS mobile device environment, please see our whitepaper: Simplifying the move from BlackBerry to Multi-OS.)

So you’ve secured the device. What about the content?

Once you have implemented mobile device management (MDM), the next mobile problem to address is information sprawl. Because they increasingly want access to more than just email, business users are taking advantage of the sharing and access capabilities of consumer mobile devices, including app-based cloud services. Workers now use smartphones and tablets as their primary computing endpoints and have high expectations for mobile collaboration capabilities. Users want to access and share everything from email to desktop files both internally and externally, and utilize corporate repositories like Microsoft SharePoint and Windows File Shares, from behind the firewall, on all their devices. As content access and control moves from IT to the individual user, a new set of opportunities—and challenges—arise:

- **Most mobile devices are consumer first—business second.** Part of their value to users is their portability, yes. But just as important is their ease of use. Locking them down damages the user experience that makes up so much of their value. As a result, most companies allow a mix of personal and corporate apps on mobile devices and impose far fewer usage restrictions.

- **Mobile devices have lots of storage.** A large amount of corporate data can potentially be stored locally on the device, giving users increased potential for productivity. And many devices come packaged with free access to cloud storage apps. This means that sensitive data can be spread far and wide.
- **Mobile devices are cloud-connected.** Consumer-focused services such as Dropbox have made it very easy to move data from the device to cloud, also enabling sharing of the data with 3rd parties outside enterprise control.
- **Mobile devices are hyper-connected.** Mobile connections are persistent. Devices try to connect constantly to any available network—corporate Wi-Fi, public Wi-Fi, or cellular—whether or not it is trusted by the enterprise.

Users demanding anywhere, anytime access to corporate information have come to expect easy and quick access based on their experience, for example, with "personal cloud services" that let them manage their favorite personal content such as photos and videos across devices. Default email and networking solutions are not flexible enough to solve most of their content access and collaboration requirements. And every new tablet or smartphone comes with various solutions to sync data with other devices at no additional cost, leaving IT with additional challenges once they have addressed device and application security and OS platform support.

An emerging priority for your Mobile First environment is extending the perimeter to corporate information on mobile devices.

It's not enough to simply secure the physical device. An emerging priority for your Mobile First environment is extending the perimeter to corporate information on mobile devices. And broadening your mobile strategy to address information sprawl.

1. Mobile First Platform: About Enterprise Mobility Management

MDM solutions are designed to set and enforce mobile management policies at the device level. Unless draconian "lockdown" is implemented, there is no inherent control of applications or content on a device. This problem is exacerbated when it is the employee's personal device in question. IT Admins who implemented "lockdown" have in many cases frustrated their power users, and faced additional problems with users "going rogue." As a result, mobile-focused IT departments are now looking to Enterprise Mobility Management (EMM) solutions, which enable management, configuration and security policy frameworks across devices, applications and content, to address the increased risk of information sprawl.

MDM solutions are designed to set and enforce management policies at the device level. Unless draconian "lockdown" is implemented, there is no inherent control of applications or content on a device.

Gartner introduced EMM as a concept in 2012. They defined it as including many of the services for optimizing and enabling mobile applications and data on the device, as well as for ensuring the security of that data. There are many vendors in the market providing a range of solutions, from point products to comprehensive platforms.

Any EMM solution assessment should include the following considerations:

- **Cross-Platform Support** End users get to use the mobile device of their choice, protected by transparent security policies. This increases end-user satisfaction and reduces corporate risk.

- **Single Management Console** Efficient policy management across platforms for devices, applications and content requires a single administrative interface. Enterprise configurations for email, Wi-Fi, VPN and consistent security polices like passcode authentication, device encryption and remote wipe across multiple platforms need to be applied, simplifying the day-to-day operations of managing a multi-platform mobile environment.

- **Enterprise-grade architecture** Although many EMM implementations begin as small pilots, most need to scale quickly. Companies need to decide on whether they want EMM solutions deployed on-premise or in a SaaS/cloud model and ensure their vendor can scale to support both device and application requirements.

- **Secure Email** The solutions should provide the option to either secure native email or provide a secure container for access to 3rd-party email apps. In addition, the ability to define email attachment encryption and data loss prevention (DLP) policy definitions needs to be present.

- **Integrated Enterprise App Storefront** How is the concept of enterprise app persona supported? How do users access their corporate content securely and natively via business apps and data on a mobile device? A built-in Enterprise App Storefront provides tight security and improves the user's discovery experience, from distribution and delivery to the whole lifecycle management of recommended and required mobile applications (in-house and 3rd-party) company-wide.

- **App Management and Security** Businesses want the ability to securely manage which mobile applications are installed on their devices. IT Administrators need to quickly select which applications are required, allowed or disallowed, and then associate these apps with rules that specify the consequences of being out of policy.

- **End-to-End Data Encryption** Consider how data encryption is supported. Is there a container functionality and encryption of all corporate data on the device? Do IT administrators have the ability to selectively wipe this data while preserving personal data if the device is lost or stolen? In addition, all corporate data-in-motion should be secured via app-specific VPN tunnels.

- **Data Loss Prevention** Are DLP controls such as copy-paste and open-in restrictions supported allowing end-users to access corporate data only via approved apps? Are these features available for both in-house applications and secure third party apps?

2. Getting Down to Business: Managing Applications and Content

In the Mobile First era, end-users want more than just secure email. They want their own devices and they want persistent access to the apps, media and online content they need to get their work done. Many of the vendors in the EMM space began by offering MDM and evolved functionality to support application and content management by offering basic versions of productivity applications like email and file sync-and-share (FSS). (For more information on MobileIron's solution, see Docs@Work: Data Loss Prevention and Secure Access.) Yet there are many strong pure play contenders in the file sync and share space that have added mobile solutions to their portfolio. Analysts agree the market is dynamic and that locking into a single solution to provide both EMM and enterprise mobile content management expertise may be premature depending on particular environments and scenarios. As a result, MobileIron has taken a platform approach, allowing 3rd-party and in-house app developers including leading FSS vendors, access to its management and security capabilities via an SDK and app wrapping technologies.

> "Email, Calendar and Contacts (Personal Information Management), mobile file syncing apps and mobile web browsers are the three basic tools most users use on their mobile devices to get a lot of their everyday work done. You can probably get 99% of your secure mobile access to enterprise solved with 1% of the effort through these three mobile Apps."
>
> **– Madden, 2013**

Leveraging the Platform: Extending MDM investment

On a mobile device, 3rd-party apps enabled with an EMM SDK or app wrapping reside and run within a passcode-protected secure container. (For more information on MobileIron's AppConnect SDK and App Wrapping solution, see AppConnect FAQ for Technology Partners.) Enterprise Management solutions secure and manage enterprise mobile apps, providing the required single pane for scalable deployments of pure play mobile content management apps by:

Distributing apps only to authorized devices

- Authentication: Confirm identity through domain username and password or certificates so only approved users can access business apps
- Single sign-on: Enforce time-based app-level sign-on across app containers
- Authorization: Allow or block app usage or storage based on device posture

Delivering app configurations and policies to apps at runtime

- Silently configure personalized settings such as user name, server name, and custom attributes without requiring user intervention

Enabling security and management features

- Encryption: Ensure that all app data stored on the device is encrypted
- DLP controls: Set data loss prevention (DLP) policies so sensitive data doesn't leave the container (i.e "open-in, copy/paste, print)
- Dynamic policy: Update app policies dynamically

Reporting analytical usage data for apps

Selective Wipe

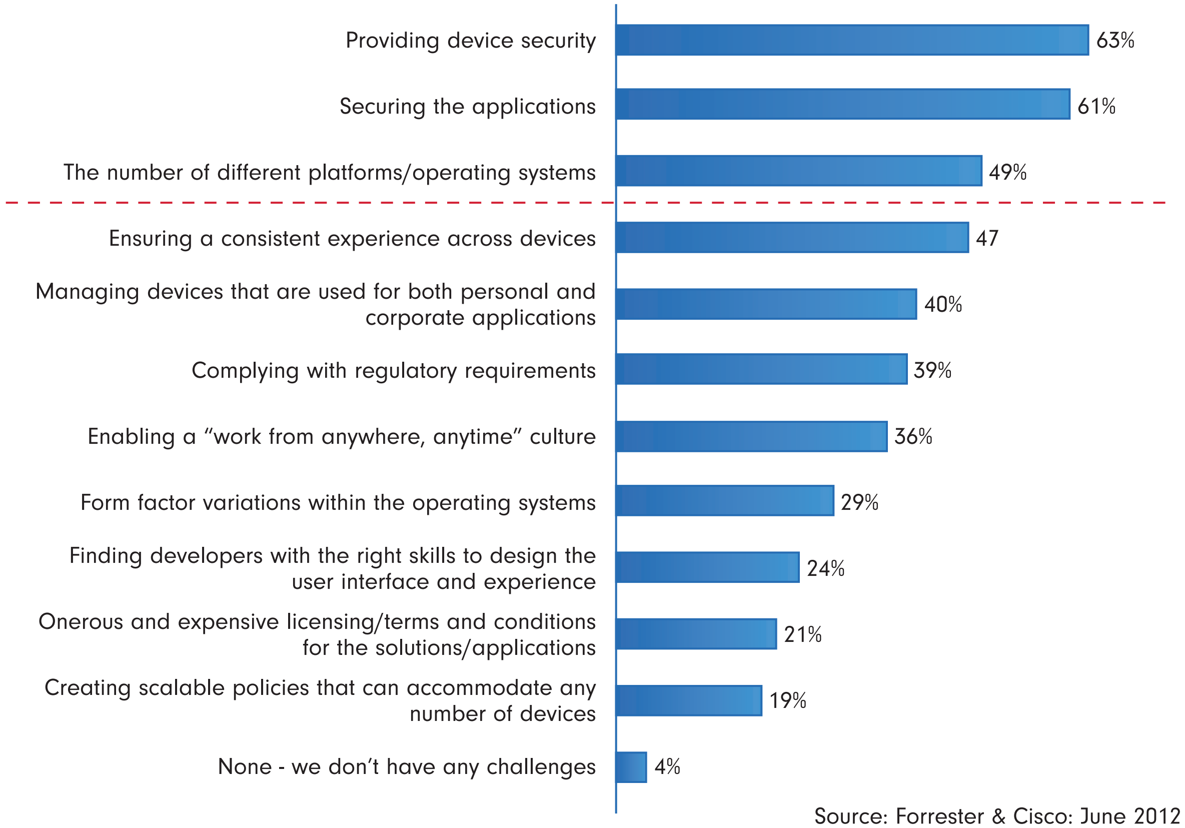
- Revoking app privileges as necessary including remotely wipe app data without touching personal data

3. Identifying the Right Mobile Content Management Partner

Both Gartner and Forrester have completed extensive reviews of file sync and share vendors and agree that when it comes to deciding on the right Mobile Content Management (MCM) solution for a particular business case it's important to remember this maxim: Employees are concerned more with usability than security. This means finding a solution that addresses corporate users' need to easily access, review and edit files, but that also meets the level of security required, is paramount.

> Finding a solution that addresses corporate users' need to easily access, review and edit files, but that also meets the level of security required, is paramount.

"What challenges, if any, does your firm face when developing and managing corporate-issued or employee-owned devices such as smartphones, tablets, or laptops?



Source: Forrester & Cisco: June 2012

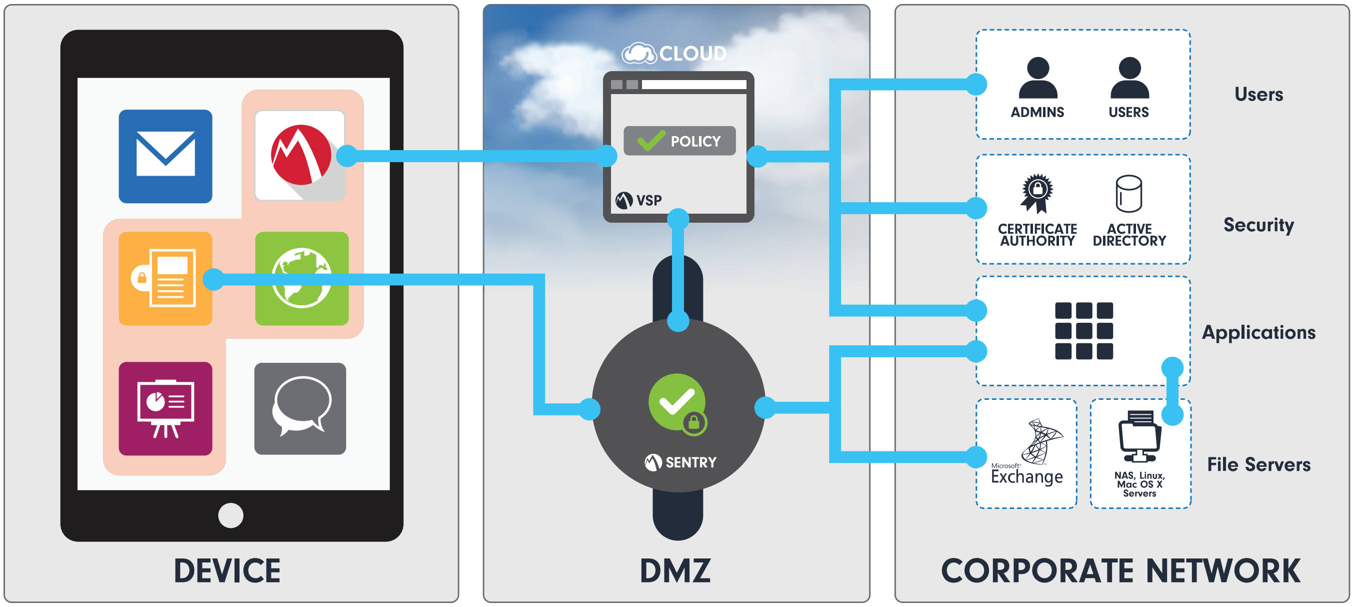
Business user requirements for mobile content access and collaboration can be summarized into 3 major functionality categories:

1. Access to current and up-to-date files without a VPN, even those stored behind the firewall
2. Ability to create, edit and annotate files securely in all formats using best-suited applications on any device
3. Ability to share files (internal and external) regardless of device type

From an IT perspective, solution suitability can be assessed against business requirements in 5 categories:

1) **Architecture – Cloud, on-premise or hybrid deployment flexibility for data and file storage and access. Is security, speed of implementation or user-experience the primary driver?**

Thanks to simplified implementation and anywhere access to content, cloud solutions are good at handling the needs of a mobile workforce and collaborating with 3rd parties (customers, partners, vendors). However, some regulated industries and enterprises in particular prefer to keep all their content behind the firewall with an on-premise solution, as on-premise deployment ensures complete control over the availability, integrity and confidentiality of information. In some circumstances a hybrid solution makes sense, with a server-side control plane in the cloud while the data is stored on-premise.



2) **MCM functionality – What are the mobile business use cases driving MCM deployment?**

MCM offerings can provide anything from basic access to PDFs on a smartphone to the full ability to create, edit, annotate, collaborate and sync in any file format on any mobile device. Matching vendor capability with the line-of-business requirements will ensure adoption. The solution should deliver, at a minimum, what the employee can get for free as a consumer. Also, users want secure, real-time mobile access to files stored in SharePoint, Windows File Shares and other Enterprise Content Management (ECM) systems behind the corporate firewall, without a VPN.

3) **Security – Finding the balance: Securing data at rest, in transit, in-use.**

As highlighted earlier, at the crux of any MCM implementation is finding the balance between usability and security. Understanding if and how the MCM solution addresses corporate requirements for secure data at rest, in transit and the security of the actual app, while providing an acceptable user experience is key. Corporate policy may require that files and content need to be tracked and security policy enforced on both managed and unmanaged devices. Ensuring audit and reporting capability is part of the compliance and security checklist. (For a detailed discussion on MCM security, see Gartner Technical Professional Advice: Enterprise File Synchronization and Sharing: Thinking Through the Security Issues)

4) Platform – Relationship in place, pure-play or strategic supplier?

Traditional file sync and share platforms have been in place for years and existing vendor relationships and investment can become an important decision factor. However, the new area of mobile content management is rich with innovation as new entrants to the market bring a mobile first approach to address requirements for access, usability and collaboration.

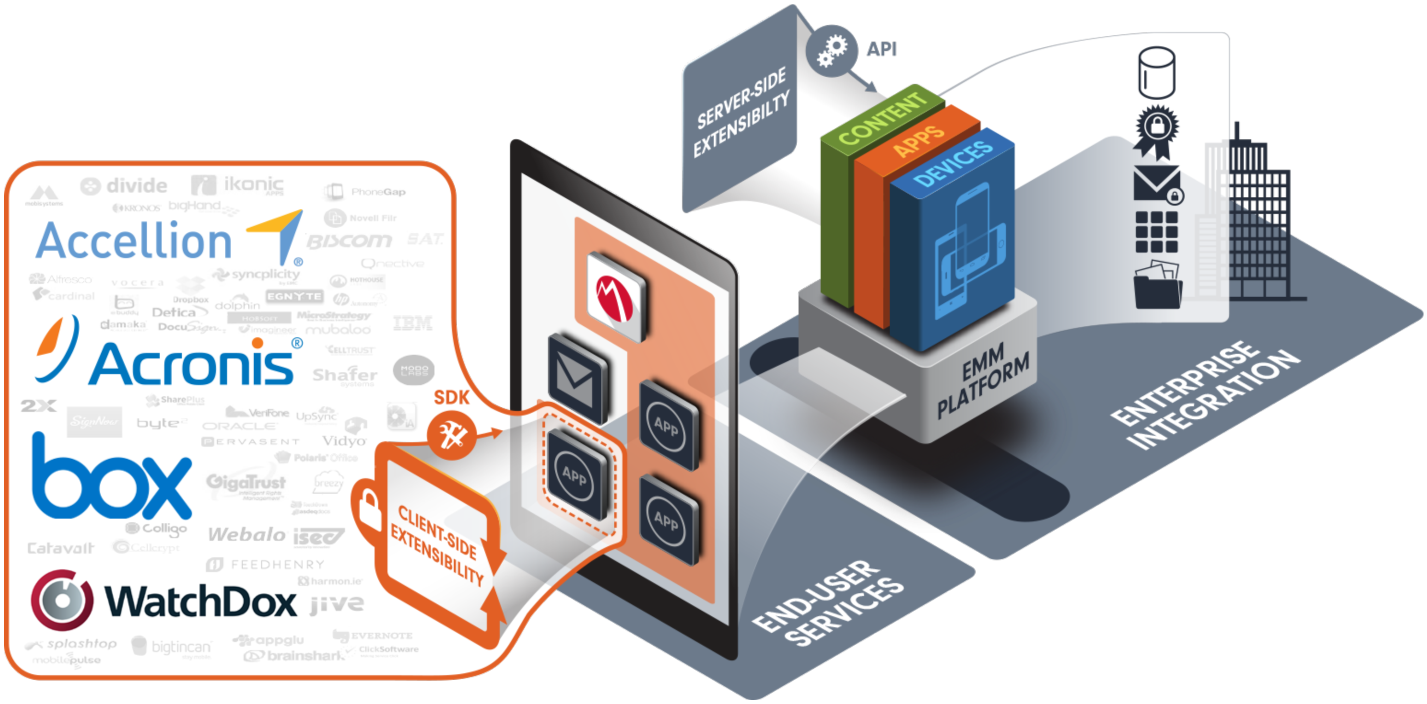
5) Price – Lower Cost or Higher functionality?

Cost is always part of the overall solution assessment and bundled functionality may seem attractive for pilot deployments. Due diligence should be paid to actual and additional costs for the term and expansion of the deployment and additional storage requirements.

4 . Securing Information Sprawl Efficiently, Without Compromise

With its extensive experience in Mobile First deployments with over 6,000 customers, MobileIron recognizes both the opportunity and advantage businesses have when extending their MDM investment, and when leveraging MobileIron's EMM platform to manage their mobile file sync and share solutions. Many organizations realize tangible cost and resource efficiencies by using MobileIron's platform to implement application-level configuration and security policy, simplifying deployment and control of their chosen mobile content solution. And as the top MCM vendors have chosen to integrate the MobileIron AppConnect SDK, customers are able to select their preferred solution without having to compromise on functionality or security.

To this end, MobileIron is profiling its integration with 4 of its partners in the AppConnect ecosystem: Accellion, Acronis mobilEcho, Box and WatchDox, to deliver best-in-class mobile content solutions. As top contenders in both Gartner and Forrester reviews, these proven MCM solutions address a range of architecture implementations . Together with MobileIron, they offer a comprehensive set of features to address any MCM deployment requirement.



5. Designing your solution

Please read the following four case studies across a range of industry sectors, for best-in-class methods to secure information sprawl. And find more information about MobileIron and our AppConnect Partners here:

http://www.mobileiron.com/solutions/mobile-content-management

Case Study: Accellion Secure Enterprise Mobility

Storage	On Premise, Hosted and Hybrid deployments
File Access	On Premise Files, Hosted and Hybrid
Security Controls	App and Data Level Security with MobileIron AppConnect SDK
Platform Support	iOS and Android
Editing and Annotation	Yes
Collaboration	Yes

A London Borough goes mobile

The London Borough of Camden saw an opportunity in BYOD. But moving forward would mean choosing the right technology partners to support seamless collaboration via devices of users' choosing, around-the-clock SharePoint access and strong security controls. They found it in MobileIron and Accellion.

"We were aware of the tremendous upside of supporting a BYOD policy, but we were also realistic about the potential risks," said Ian Lawrence, IT Manager for Camden. "That's why we outlined our must-have usability, security and compliance requirements that had to be met in order to move forward."

A key first step was automating the management of the wide range of mobile devices and associated applications that would enter the organization. The Borough decided to deploy MobileIron's Mobile Device Management (MDM) platform and MobileIron AppConnect™ to handle the inventory, delivery and user access privileges of mobile applications organization-wide. But then the pressing question was how to allow employees to access key documents and conduct business via mobile devices—as easily as working from a PC—without sacrificing needed security and control?

Armed with its list of requirements, the Borough turned to a trusted third party—mobility and wireless experts at Qolcom—for platform recommendations. Accellion's secure mobile file sharing topped the list. After an extensive in-house evaluation, Camden agreed that Accellion was the only vendor that met all of its requirements and more.

Solution

With the support from Qolcom, Camden deployed Accellion to support its transition to BYOD and CYOD. The project is undergoing a phased rollout beginning with key executives, followed by the next level of management and then remaining employees. Now employees access and collaborate on important documents via iOS and Android smartphones and tablets, whenever and wherever needed.

Thanks to Accellion's enterprise content connectors, which provide secure, real-time mobile access to files stored in SharePoint and other Enterprise Content Management (ECM) systems without a VPN, SharePoint continues to serve as the Borough's trusted content source. Users can easily and securely check documents in and out of SharePoint from a mobile device without loss of encryption or breaches in data security. And, with Accellion's mobile apps for MobileIron AppConnect™, the organization has its much needed mobile security, including user authentication, the ability to block application usage at an individual or global level and the option to deauthorize apps and remotely wipe devices if any are lost or compromised.

Case Study: Acronis mobilEcho with MobileIron

Giving a homebuilder a secure foundation

A large national homebuilder was faced with a challenge: how to enable their impressive growth, maintain tight collaboration across regions and not put critical data at risk?

At the leadership level, the company is constantly exploring and implementing ways to lower costs, improve speed to market and ensure responsive customer service. A full-blown Mobile First implementation for their field services team is the latest example of creative thinking coming from the CIO office.

One challenge they needed to address was that field services teams - which are always on the move - need to make decisions impacting inventory, supply, design and other resources. Ensuring they have what they need to make the right decision while keeping the rest of the widely dispersed team informed is no small task. The CIO already replaced laptops with iPads, enabling ease of deployment and security with MobileIron. He now needed a secure, efficient and simple way to deliver full access to corporate files on the iPad.

Acronis mobilEcho, integrated with MobileIron AppConnect, provided the secure and streamlined access to enterprise content that the team needed. All the configuration and deployment can be managed via the MobileIron console, so remote field teams just had to tap on the app to access all the documents they needed to get their work done. Making edits and annotations was easy, regardless of file type. And files could be updated and shared in real time.

With MobileIron and Acronis mobilEcho, they've found a way of working that ensures they can stay at the forefront of their business.

Acronis®

Storage	On Premise
File Access	On Premise Files
Security Controls	App and Data Level Security with MobileIron AppConnect SDK
Platform Support	iOS and Android
Editing and Annotation	Yes
Collaboration	Basic file/folder link for internal user sharing

Case Study: Box MCM with MobileIron

Sally Beauty puts a new face on its sales team

Seeking to increase the effectiveness of its field sales staff while helping them present a more professional image, Sally Beauty implemented the MobileIron enterprise mobility management (EMM) platform. Sally Beauty uses MobileIron to let retail and traveling sales staff access product collateral on iPads, recommend and deliver the most helpful apps, empower field sales reps to take orders on iPads and reduce printing costs.

In the beauty supply business, image may not be everything—but it means a lot. When Sally Beauty evaluated the way its laptop-toting sales reps were interacting with clients, the company realized it needed to not only help increase their efficiency, but also enhance the impression they were leaving on salon owners.

It wasn't difficult for Sally Beauty's IT organization to come up with a viable solution: the iPad. By distributing the device to mobile sales staff as well as in-store employees, the company knew it could boost the effectiveness and image of its customer-facing employees. But first, Sally Beauty needed a way to secure and manage these devices. Parker did his homework before selecting MobileIron.

"MobileIron came with the reputation of respecting the iPad user experience. That means we can let employees use their company-issued devices for business and personal use without letting security get in the way," says Mobility Manager Clay Parker. "We also appreciated that we could pay for our MobileIron subscription on our AT&T phone bill. One less thing to think about!"

A key plank of Sally Beauty's mobile strategy is to connect employees with the apps they need, so they won't have to waste hours searching app stores. By making frequent use of Box, a secure content sharing platform, Sally Beauty has dramatically streamlined the task of managing and distributing product information from its vendors.

"Box gives us one central location for all of our product content," Parker explains. "By creating vendor-specific folders and then inviting our vendors to manage their own collateral, we've taken the headache out of content management on our end while giving our reps the power to find exactly the right materials with a simple search."

Having the information they need at their fingertips isn't just helping Sally Beauty employees look and feel more confident—it's also boosting the company's bottom line. By distributing product collateral to 4,000 stores digitally instead of printing and mailing it, Sally Beauty is achieving measurable savings.

Storage	Cloud
File Access	Cloud and On-Premise
Security Controls	App and Data Level Security with MobileIron AppConnect SDK
Platform Support	iOS
Editing and Annotation	Yes via Box Ecosystem
Collaboration	Yes

Case Study: WatchDox Mobile Content Management with MobileIron

Financial firm protects it's own investment

Blackstone is a premier global investment and advisory firm that strives to provide solutions that create lasting value for its investors, its portfolio companies and society at large. As a leader in alternative assessment management, Blackstone preserves and protects more than $190 billion in assets.

Nevertheless, Blackstone is like a lot of modern enterprises. Its employees want to use their own mobile devices to be productive when they're onsite and off, and to collaborate with partners, customers and each other. And like other global companies in many industries, Blackstone deals with highly sensitive information. While its staffers want mobile productivity, its executive team demands security. They finally decided not to choose productivity or security. They needed both.

"The iPad is really the most convenient way to consume these documents," says Bill Murphy, CTO and managing director at Blackstone. "The percentage of iPads to employees will continue to go up based on the number of iPads we're adding each month. My gut is that it will go from 600 to more than 1,000 in the next year."

Blackstone spent a lot of time and energy finding ways to secure confidential documents on BYOD iPads, even looking at purchasing iPads for employees.

To make sure Blackstone could have its mobile productivity cake and secure it too, the company reached out to WatchDox and MobileIron, which delivers security and management for mobile apps. Blackstone chose MobileIron to manage corporate-owned and BYOD devices, and WatchDox to secure data at the document level before it is shared with any other recipients.

MobileIron enables central control of devices used to access the corporate network and resources, enforcing passwords and supporting Blackstone's complex password requirements. "We can track the device and expire it from afar when it connects to the Internet. This really shrinks down the ability for someone to attack that device to a very small window. We feel comfortable that no company confidential information is going to get stolen," says Murphy.

The WatchDox system builds access control, tracking and revocation capabilities into Blackstone documents, securing the data as opposed to trying to control the space in which it travels. This feature distinguished WatchDox as an ideal security solution for Blackstone.

WatchDox

Storage	Cloud, On Premise and Hybrid
File Access	On Premise Files
Security Controls	App and Data Level Security
Platform Support	iOS and Android
Editing and Annotation	Yes
Collaboration	Yes, File and Folder Sharing

With WatchDox and MobileIron, Blackstone can facilitate the secure, appropriate sharing of and access to critical information with internal and external stakeholders while protecting sensitive board member and senior executive communications. These safeguards allow the company-wide use of mobile devices, like iPhones and iPads, for viewing and annotating highly sensitive documents, such as investor statements and financial results.

References

Enterprise Mobility Management, Jack Madden (2013)

Gartner
Marketscope for Enterprise File Synchronization and Sharing (Feb 2013)

Forrester
The Forrester WaveTM: File Sync and Share Platforms Q3 2013 (June 2013)

Forrester & Cisco
The Next Generation Workspace Will Revolve Around Mobility and Virtualization (June 2013)

The Mobility Trust Gap
http://www.mobileiron.com/sites/default/files/whitepapers/files/Mobile-Trust-Gap_MobileIron-White-Paper.pdf

Simplfying the Move from BlackBerry to Multi-OS
http://www.mobileiron.com/whitepaper/future-mobile-device-management

MobileIron AppConnect FAQ for Technology Partners
http://info.mobileiron.com/rs/mobileiron/images/appconnect_faq.pdf