Accellion®

Enterprise Mobility Management: A Data Security Checklist

Executive Summary

Secure file sharing, syncing and productivity solutions enable mobile workers to access the files they need from any source at any location easily and securely, while ensuring that all file access and file sharing complies with the organization's policies and any applicable industry regulations. These solutions impose pressing technical and operational challenges on organizations ranging from SMBs to large enterprises.

This document presents a checklist of features organizations should review when evaluating a data security solution as part of an enterprise mobility management strategy. The features are organized into the following categories:

- Security
- User Experience
- File Access
- File Delivery
- Mobile Productivity
- Administrative Control
- Deployment Models
- Scalability
- Integration with Enterprise Content Management (ECM) platforms such as Microsoft SharePoint
- Integration with Enterprise Infrastructure System Management

The New Mobile-First Enterprise

Across every industry, the workforce is using mobile devices to help increase productivity. Employees are now using smartphones, tablets, and laptops for their daily work, leading to increased responsiveness and output. In many cases, employees are using their own personal mobile devices for work, usually with the permission of their employers. As of early 2013, nearly three-quarters of businesses worldwide have formally adopted Bring Your Own Device (BYOD) policies, expressly permitting employees to use their personal mobile devices like Android phones and iPad tablets for work.[1]

Mobile workers can now simply be called workers. Typically they carry a variety of mobile devices: 2.9 devices on average, according to a survey iPass conducted in 2013.[2] Carrying a smartphone and a tablet or laptop is a popular combination. The devices might be running different operating systems. For example, a worker might have an Android smartphone, an iPad, and a Windows laptop.

Finding themselves carrying multiple devices and needing their files on all those devices, workers have been searching for a fast, easy way to share files across devices and with other users. They want to automatically copy or “sync” files to all their devices, so the files that matter to them are always at hand. And they want an easy way to share files with internal and external colleagues, most of whom are also carrying multiple devices.

To solve this problem, many turned first to free solutions like Dropbox, which sync files without any oversight or controls by the IT department. Unfortunately, these services are becoming famous for their security breaches. For example, Dropbox once disabled all password protection for all files in all accounts for about 4 hours.[3] After auditing its network for data leaks, IBM banned Dropbox and another file-syncing service, Evernote, from its employees’ systems.[4] When implementing secure file sharing solutions, organizations need more control and visibility than services like Dropbox seem capable of providing.

Mobility and convenience should not become excuses for mitigating or dismissing security standards. Whether users are working on desktop systems or the latest smartphone, organizations need to be able to enforce the same data security policies and controls they are used to enforcing with traditional file servers and LANs. They need to be able to set access controls defining which users can access which files and in which locations. Confidential data must remain confidential, and user activity must be monitored and tracked, just as security policies and industry regulations like HIPAA require.

In fact, rather than lowering security standards for mobile users, organizations should raise them. Files on mobile devices are at risk of interception when transmitted over public Wi-Fi hotspots, and they are vulnerable to infection from new forms of mobile malware, many of which take advantage of the lax security found on most smartphones and tablets. Mobile users often leave security features turned off, and many fall behind with operating system upgrades, leaving their devices more vulnerable to attack.

Malware in a particular is a growing risk for mobile users. IBM estimates that these new forms of attack are growing 15% annually.[5] Other observers have found evidence that mobile malware,

[1] According to The iPass Global Mobile Workforce Report for Q2 2013, 74.6% of organizations in the U.S. support BYOD policies. Globally, 70.3% of organizations support BYOD. Thirty-five percent of workers said that an employer’s position on BYOD might affect whether or not they accepted a job offer. http://www.ipass.com/wp-content/uploads/2013/06/ipass_mobile-workforce-report_q2_2013.pdf

[2] http://www.ipass.com/wp-content/uploads/2013/03/ipass_mobile-workforce-report_q1_2013.pdf

[3] http://techcrunch.com/2011/06/20/dropbox-security-bug-made-passwords-optional-for-four-hours/

[4] http://www.computerworld.com/s/article/9227888/Mobile_devices_bring_cloud_storage_and_security_risks_to_work

[5] http://www.computerweekly.com/news/2240105733/Mobile-malware-is-on-the-rise-warns-IBM-report

especially for the Android operating system, is growing at much brisker pace—up 614% in 2012 alone.[6]

New Challenge for Organizations

Mobile file sharing, syncing, and collaboration solutions impose pressing technical and operational challenges on organizations ranging from SMBs to large enterprises. Data must be secure. File sharing among both internal and external users must adhere to company policies and industry regulations. At the same time, employees need fast, convenient access to content to be productive. File sharing must support all the various file types that users work with, ranging from Microsoft Office files, PDFs, and multi-gigabyte files used in advertising, engineering, and healthcare. File sharing must work across devices and across device architectures: from iPhones to Android tablets to Windows desktops.

In short, mobile-first organizations need secure file sharing, syncing and productivity solutions.

Secure Mobile File Sharing, Syncing and Productivity Solutions Defined

An IT solution that enables mobile users to:

- Access all the files they need for work, including files stored on file servers, and Enterprise Content Management systems such as Microsoft SharePoint.
- View, edit, and save these files on mobile devices in compliance with access controls defined and enforced by IT administrators.
- Distribute or "sync" these files across all authorized devices, including smartphones, tablets, laptops, and desktop systems, including personal devices approved for work as a part of a BYOD policy.
- Send files in a secure point-to-point fashion to other authorized users.

Secure file sharing, syncing and productivity solutions enable mobile workers to access the files they need from any source at any location easily and securely, while ensuring that all file access and file sharing complies with the organization's policies and any applicable industry regulations.

The remainder of this document presents a checklist of features that SMBs and large enterprises should look for in a solution. The features are organized into the following categories:

- Security
- User Experience
- File Access
- File Delivery
- Mobile Productivity
- Administrative Control
- Deployment Models
- Scalability
- Integration with Enterprise Content Management (ECM) platforms such as Microsoft SharePoint
- Integration with Enterprise Infrastructure
- System Management

[6] http://www.eweek.com/security/android-malware-climbs-614-percent-in-2012-study/

The Mobile Content Security Checklist

Security

The solution should protect the confidentiality and integrity of files on mobile devices and in transit. The security controls should be rigorous enough to support compliance with industry regulations such as the Healthcare Insurance Portability and Availability Act (HIPAA) and Sarbanes-Oxley (SOX).

- **Secure containers**
  The solution should provide protected storage areas, known as "secure containers," to protect files on mobile devices from unauthorized access and from malware contamination by other files on the device. All files in secure containers should be encrypted and accessed in a separate secure memory space available only to authorized apps. (See "Mobile app whitelisting" below.) IT administrators should be able to track and manage all files in secure containers.
- **Encryption at rest and in transit**
  The solution should apply industry-standard encryption to protect data at rest on servers and mobile devices and in transit to and from end points.
- **Ownership of encryption keys**
  Ownership of the encryption keys used to encrypt data should reside with the enterprise, not with the solution vendor. At all times, enterprises should have full access to their data and control the means of that data being encrypted.
- **FIPS 140-2 Certification (Encryption)**
  To allow use by U.S. federal agencies, the solution should support FIPS 140-2 certified encryption.
- **Workspace-specific access controls**
  The solution should also support workspace-specific access controls, so that permissions for workspaces can easily be assigned to teams or departments.
- **AV protection**
  The solution should provide real-time malware scanning of content each time a file is uploaded or downloaded. Malware-infected files should be automatically quarantined and prevented from being uploaded to shared workspaces. The AV scanning feature should automatically update itself with new signature files when new forms of malware are reported by security researchers.
- **Support for remote wipe**
  The solution should enable authorized administrators to remotely delete content from specific mobile devices. If an employee leaves an organization, administrators should be able to remotely delete that employee's content from every mobile device under management. If a device is lost or stolen, administrators should be able to promptly delete all enterprise content on that particular device and prevent it from accessing enterprise resources such as file servers in the future.
- **Mobile app whitelisting**
  The solution should support a whitelist of mobile apps approved by the IT organization. Only mobile apps on the whitelist should be allowed to open, view, or edit files managed through the solution.
- **Support for prevalent mobile platforms (Android, iOS, Windows)**
  The solution should support the most popular mobile platforms in use by businesses and government agencies, including Android, iOS, and Windows.
- **Data sovereignty support**
  Administrators should be able to control the physical storage location of specific workspaces and files for specific users. For example, IT Administrators should be

able to ensure that files belonging to German users are stored in Germany, while those belonging to American users are stored in the U.S.

User Experience

In too many enterprise software solutions, security comes at the expense of usability. Many systems prized for their security are cumbersome, especially on mobile devices. To be widely adopted, a mobile file sharing, syncing and productivity solution should be easy—even fun—to use, requiring minimal learning even for non-technical users, while applying rigorous security controls to protect users, devices, and content.

- **Modern and intuitive user interface**
  The solution should take advantage of the latest advances in UI design to make mobile collaboration and file sharing easy and intuitive.
- **"Mobile-first" design.**
  The solution should be designed first and foremost to work on mobile devices, which for many workers have become the primary interface for online collaboration and access to enterprise data. A "mobile-first" design takes into account the small screens and online keyboards of many mobile devices, and works with a variety of screen sizes, resolutions, and shapes. Processes should require the minimum number of steps. Interface elements should be legible on small screens. Interactive elements should follow paradigms commonly used in today's mobile apps.
- **Consistent user interface (UI) across mobile devices, Web applications, and desktop systems**
  The solution should provide a consistent visual and operational paradigm across all its platforms, including mobile devices, Web applications running in browsers, and desktop systems. Users should not have to puzzle over how the solution works in a browser compared to how it works on a desktop system or a smartphone.
- **Integrated online help**
  The solution should include online help, so users always have useful intructions and explanations at their fingertips. Besides improving user experiences and productivity, comprehensive online help has the added benefit of reducing training requirements and help desk workloads.

File Access

File Access ensures that employees always have access to the content they need, even on smartphones and tablets.

- **Secure workspaces for files being accessed remotely**
  The solution should provide secure workspaces for files, so that multiple authorized users can access files and saved them to a common secure repository.
- **Sync for workspaces – real-time or on-demand**
  The solution should enable mobile users to sync files with workspaces either automatically in real time (whenever a file is added, removed, or changed) or on demand.
- **Support for common file types, including Microsoft Office and PDF**

The solution should enable users to view, edit, and share common file types, such as Microsoft Office files (including Word, Excel, and PowerPoint) and Adobe PDF.

- **Integration with ECM systems**
  The solution should integrate with popular Enterprise Content Management systems, such as Microsoft SharePoint and Documentum, so that authorized users can directly and securely access content within these systems from mobile devices, without requiring a VPN connection.
- **Support for working offline**
  The solution should enable authorized users of mobile devices to view and edit enterprise content on mobile devices even when those devices are not connected to a network.
- **Versioning**
  The solution should automatically assign a unique version number to each revision of a file under management, so that users can distinguish one revision from other and quickly determine whether or not they are accessing the latest version of a file.
- **File commenting and group discussions**
  When accessing files from a remote location, it’s important for users to be able to understand the context of a file and the reasoning behind any recent changes to content.
- **Secure workspaces**
  The solution should provide secure workspaces where authorized users can post, edit, and share files. The workspaces should limit file access to authorized users and protect files with encryption.

File Delivery

File Delivery enables authorized users to share content with other users in a secure and controlled environment.

- **File size limits**
  The solution should support file sizes beyond the traditional 10 MB of enterprise email. In many use cases and industries such as advertising, engineering, and healthcare, it’s not unusual for file sizes to reach several gigabytes. The solution should support the secure transmission and management of files larger than 4GB, preferably unlimited in size.
- **Return receipts**
  The solution should enable senders to receive electronic receipts indicating that files they have sent to other users have been received and viewed.
- **Disallow forwarding**
  Users should have the option of preventing the files they are sending from being forwarded to other users. When this option is selected, message recipients will be able to open files but not forward them.
- **Request file for secure delivery (including files from external users)**
  Authorized users should be able to provide other users, including external users, with a mechanism for securely sharing files. An internal user should be able to request a file from an external user, and the external user should be able to securely send the file without requiring an account on an internal directory such

as LDAP or Active Directory. The transfer of the file should be able to be monitored and control by IT administrators.

- **SFTP support**
  The solution should optionally support the Secure File Transfer Protocol (SFTP), eliminating the need for a separate SFTP server. Supporting SFTP helps centralize the security and management of all files being shared.

Mobile Productivity

Mobile Productivity ensures that employees always have access to content and collaboration tools they need to be productive, even when working exclusively on mobile devices.

- **Ability to access files**
  Mobile users should be able to access the files they need easily and securely.
- **Ability to annotate PDFs**
  Mobile users should be able to annotate PDF files and to share annotated files quickly, easily, and securely with other authorized users.
- **Ability to edit Microsoft Office files**
  The solution should enable users to edit files, including standard Microsoft Office files, on mobile devices without having to first replicate the files.
- **Ability to move files across workspaces, clouds, and ECM systems**
  Authorized users should be able to move files across secure workspaces, clouds, and ECM systems. For example, an authorized user should be able to move a file from a secure workspace to a SharePoint server, or from one Windows File Share to another. Users should be able to select files and to navigate through storage areas in an intuitive manner, even from small-screen devices like smartphones.
- **Threaded discussions tied to file revisions, providing context for content**
  The solution should enable users to participate in threaded discussions about files stored in workspaces, so that users can understand why and how files are being authored, edited, and used.
- **Activity stream so users can understand their colleagues' work on the content that matters to them**
  The solution should include a micro-blogging function that reports automatically generated status updates so users can track work on the content that matters to them.
- **Support for cross-boundary communication with trusted external users**
  Authorized employees should be able to exchange messages and files securely with trusted external users, such as customers and partners who do not have email or ECM accounts in the enterprise.

Administrative Control

Administrative Control gives IT administrators visibility into and control over all mobile file-sharing activities.

- **Centralized control over accounts and files**
  The solution should centralize administrative control over all user accounts, workspaces, and files in the system.

- **Real-time administrative dashboards**
  Administrators should be able monitor system activity and status through real-time dashboards available only to authorized administrators.
- **Mobile access to administrative console**
  Administrators should be able to access the solution's administrative console—including dashboard reporting, policy controls, and system configuration tools—securely from mobile devices and desktop systems.
- **Logging: visibility into which users have accessed which files when**
  Administrators should be able to determine which users have accessed any file, when, and how often. They should be able to confirm that files whose content is covered by industry regulations such as HIPAA and SOX have been managed in accordance with those regulations.
- **Fine-grained access controls: policies can limit who can view and who can edit specific files**
  Administrators should be able to define and enforce access controls for specific files and specific users.

Architecture and Deployment Models

Deployment Models should include on-premise and hosted solutions, offering organizations a range of options for optimizing security, operational costs, and scalability.

- **Private cloud**
  To minimize the risk of data leakage or service outages from public clouds, the solution should be deployable on a private cloud under the complete control of the organization's IT department.
- **On Premise**
  The solution should be deployable on an on-premise private cloud, offering complete control over the availability, integrity, and confidentiality of data. The solution should support popular private-cloud platforms such as VMware, Citrix XenServer, and Microsoft Hyper-V.
- **Hosted**
  Private cloud hosted deployment provides the flexibility and scalability of a managed service offering while ensuring high levels of security and control.
- **Hybrid cloud**
  The solution should also support increasingly popular hybrid cloud architectures, seamlessly spanning on-premise private clouds and hosted environments to provide an optimal combination of security, control, and flexibility.
- **Multi-tier architecture**
  The solution should feature a modular architecture, enabling functionality to be divided into multiple tiers for increased security and scalability. Industry best practices typically call for a presentation tier, an application tier, and a database tier. Each tier should be able to be placed anywhere in the network (for example, the presentation tier in the DMZ, while the application and database tier reside behind the internal firewall). Furthermore, each tier should be able to scale independently to meet the specific workload requirements of the enterprise using the solution.

Scalability

Data volumes are growing, and the number of mobile devices in the enterprise continues to multiply. Organizations should be able to scale their deployment easily and cost-effectively.

- **Horizontal and vertical scalability**
  The solution architecture should allow it to scale from small single server deployments all the way to global multi-location deployments. The solution should be able to support hundreds of thousands of users on the system.
- **Centralized management of appliances**
  The solution should centralize the management of all its virtual and hardware appliances, so that Secure Mobile File Sharing can be easily scaled in a manageable way.
- **Intelligent replication through rules or locations**
  To facilitate scaling the solution, administrators should be able to easily replicate rules, policies, and local content when deploying new appliances.

Integration with Enterprise Content Management (ECM) Platforms such as Microsoft SharePoint

Enterprise Content Management systems help businesses store, organize, and protect files. The most popular ECM platform, Microsoft SharePoint, is used by over 78% of the Fortune 500.[7] Other ECM platforms like Documentum are popular as well. By integrating Secure Mobile File Sharing with ECM systems, IT organizations can bring ECM content and ECM security policies to the mobile workforce.

- **VPN-less mobile access to ECM files**
  Mobile users should be able to access files stores in ECM systems such as Microsoft SharePoint securely and directly through their mobile devices without requiring a VPN connection.

- **Maintain ECM as system of record**
  If ECM administrators want to maintain an ECM platform as the system of record, they should be able to ensure that files are saved only to the ECM platform, not to other file shares.

- **External sharing of ECM files**
  Users should be able to share ECM files with authorized external users, if allowed to do so by security policies.

Integration with Enterprise Infrastructure

Secure solutions should integrate with important IT services such as user directory services, single sign-on services, and Data Loss Prevention (DLP) systems in order to streamline operations and reduce operational overhead.

- **Integration with LDAP and Active Directory (AD)**
  The solution should integrate with industry-standard directory services such as LDAP and Active Directory. Organizations should not have to maintain a separate directory system just for Secure Mobile File Sharing if they have other standard directories services in place.

[7] http://technet.microsoft.com/en-us/magazine/gg981684.aspx

- **Integration with Single Sign-On (SSO) services**
  The solution should integrate with industry standard single sign-on services such as those based on SAML, Kerberos, and LDAP. Organizations that have deployed single sign-on services should not have to maintain a separate sign-on service for file sharing.
- **Integration with DLP systems**
  The solution should integrate with industry-standard DLP services so that mobile file sharing adheres to an organization's existing DLP policies.
- **Integration with Mobile Device Management (MDM) systems**
  With an MDM solution in place, there is an added layer of device protection. The solution should integrate with popular MDM systems to simplify the provisioning, management, and securing of mobile devices accessing an organization's files.
- **Plugins**
  To simplify access to Secure Mobile File Sharing and discourage users from seeking unmanaged and unmonitored channels for distributing files, the solution should offer plug-ins for popular communication applications including Microsoft Outlook and Microsoft SharePoint.

System Management

System Management features help IT administrators ensure that content is managed and archived according to an organization's security and data retention policies, that software is properly configured and updated, and that an organization's data is store in a continuously monitored, autonomous repository.

- **Auto-updates**
  The solution should automatically update client software on mobile devices.
- **Storage monitoring**
  Administrators should be able to monitor the use of file storage across devices and servers.
- **Separate storage per account**
  Even in a hosted deployment, organizations should be able to ensure that their data is stored separately from that of other organizations.

Conclusion

Secure file sharing, syncing and productivity solutions enable mobile workers to access the files they need from any source at any location easily and securely, while ensuring that all file access and file sharing complies with the organization's policies and any applicable industry regulations.

Pressing technical and operational challenges associated with data security can be addressed through careful review of key considerations that should be part of an organization's mobility management strategy.

About kiteworks

kiteworks by Accellion is a next generation mobile solution that improves business productivity by enabling users to securely and seamlessly access, create, edit, and share content from any device anytime, anywhere.

Corporations and government agencies around the world have chosen secure mobile file sharing solutions from Accellion to improve business productivity. With kiteworks, organizations now have a streamlined user interface, and increased scalability, which enables their employees to work securely, wherever.

Related Resources

- **kite**works datasheet
- Gartner MarketScope: Enterprise File Sync and Share
- 5 Best Practices for Secure Enterprise Content Mobility

About Accellion

Accellion, Inc. is an award-winning private company that provides mobile solutions to enterprise organizations to enable increased business productivity while ensuring data security and compliance. As the leading provider of private cloud solutions for secure file sharing, Accellion offers enterprise organizations the scalability, flexibility, control and security to enable a mobile workforce with the tools they need to create access and share information securely, wherever work takes them. More than 12 million users and 2,000 of the world's leading corporations and government agencies use Accellion solutions to increase business productivity, protect intellectual property, ensure compliance and reduce IT costs.

Email: sales@accellion.com
Phone: +1 650 485 4300

Accellion, Inc.
1804 Embarcadero Road
Palo Alto, CA 94303

For additional information: www.accellion.com/resources/whitepapers

Accellion®