The Top Five Security Challenges Presented by Mobile SharePoint Access

and how they are addressed by Colligo Briefcase Enterprise

The flood of iPads and iPhones into the enterprise brings huge productivity gains for the mobile workforce, but introduces a raft of security concerns for the IT department. The line between home and office, personal and corporate, has been blurred. Mobile devices with SharePoint access are attractive targets for attackers, as they can potentially gain access to an entire enterprise network.

With this in mind, we designed Colligo Briefcase Enterprise with enterprise-class security as a priority. This white paper outlines the top five questions executives are asking about secure mobile access to SharePoint, and explains how they are addressed by Colligo Briefcase Enterprise.

Colligo Briefcase Enterprise: The simplicity of iPad, the security of SharePoint

Designed from the start with enterprise security as a priority

Security sets Colligo Briefcase Enterprise apart from other mobile SharePoint solutions. We set out to design a solution that would be as easy-to-use as consumer file sharing products, with the familiarity of SharePoint underpinned by enterprise-class security. Our design goal was to make enterprise SharePoint content easy for mobile iPad and iPhone users to access, while ensuring that sensitive corporate data is encrypted, locked, and removable on demand.

1: What happens when an iPad or iPhone is lost or stolen?

Colligo Briefcase Enterprise has its own passcode access

In addition to the device passcode, Briefcase has its own separate passcode. It looks and behaves just like the usual iOS 4-digit passcode system.

After 10 failed logins, content is auto-wiped

If someone attempts to break into Colligo Briefcase Enterprise by brute force, the app will auto-wipe all stored content after 10 failed login attempts. To avoid inadvertent auto-wipe for a legitimate user who has simply forgotten their password, each re-attempt is presented with increasing delay. Once a wipe is triggered, the data is immediately removed.

SharePoint content can be remotely wiped from the device

If a device is lost or stolen, an administrator can remotely wipe the SharePoint content from the device. The wipe is triggered as soon as the device is online and establishes a link to receive a push notification. Note: This functionality is provided by a Mobile Device Management (MDM) system in conjunction with Colligo Briefcase Enterprise. Most MDMs will allow a selective wipe, enabling deletion of all corporate data, but leaving personal data intact. (This is most often used when an employee leaves the company, taking their personal device with them.)

A stolen iPad or iPhone can also be remotely wiped through iCloud

If a device is stolen, it can also be remote-wiped using iCloud (iOS5 and up).

2: How can I control access to SharePoint content?

Administrators can restrict access on a site-by-site basis

For enterprises requiring granular management of SharePoint access on mobile devices, Colligo Administrator is an administration suite that provides complete control at the user or group level. SharePoint site and list access and caching permissions can be centrally configured and deployed, with no configuration required by end users. Through Colligo Administrator, content can be added or expired on a user's device at any time, and the entire cache can be wiped remotely.

Metrics determining SharePoint adoption and ROI can also be tracked, communicated, and optimized through Colligo Administrator. These metrics not only help to determine usefulness of content within the organization, but can also be used to spotlight suspicious peaks in activity on highly sensitive documents.

Sharing highly sensitive corporate documents can be restricted

Using Colligo Administrator, sharing highly sensitive corporate data externally can be restricted. See Question Five for more detail.

Colligo Briefcase Enterprise supports all SharePoint authentication methods

Colligo Briefcase Enterprise supports all SharePoint authentication methods, from claims-based to classic mode. Colligo Briefcase Enterprise's design leverages the security and familiarity of SharePoint, while employing the intuitive UI elements of the iPad and iPhone, such as touchscreen and swipe. Our goal was the ultimate in usability, with no compromise on security.

3: What if a malicious app or person tries to access corporate documents?

All stored data is encrypted with AES 256-bit hardware encryption

Colligo Briefcase Enterprise uses AES 256-bit encryption for all stored data. This is the highest form of encryption available and cannot be disabled by users.

Colligo Briefcase Enterprise uses the device's Keychain to protect users' SharePoint credentials

SharePoint credentials are needed in order to sync iPad or iPhone content. Each user's SharePoint credentials are encrypted with AES 256-bit encryption and then stored in the device's Keychain, the highest form of trust-chain security. The Keychain is an encrypted key store that provides protection of sensitive data outside of the app data area. Access to the Keychain is controlled by iOS. If access to the Keychain needs to be revoked, it can be achieved simply by removing the device's provisioning.

Screen capture is prevented with screen blanking

One security flaw that is often overlooked is the ability of a rogue app to use the iPad's screen capture capabilities. Colligo Briefcase Enterprise prevents rogue screen capture by simply blanking the screen when changing applications.

Colligo Briefcase Enterprise detects alteration of configuration p-list files and performs reset

Colligo Briefcase Enterprise will detect any modification to the p-list (.plist) files on the iPad and will remove all data and configurations, effectively resetting the app, as if it had been deleted or freshly installed.

Colligo Briefcase Enterprise does not back up any app data on iTunes

Colligo Briefcase Enterprise interacts securely with SharePoint to sync and cache content on the iPad or iPhone. Data is kept securely within SharePoint and in encrypted form within Colligo Briefcase Enterprise. Data does not leave these secure confines and is never backed up on iTunes, preventing other potential security breaches.

"Colligo Briefcase Enterprise provides the most secure, robust and easy-to-use solution for accessing, syncing and viewing SharePoint content on an iPad."

David Britton, Applications Manager, Global 100 law firm, Allens Arthur Robinson

Allens Arthur Robinson

4: What if a jail-broken iPad appears on the network?

Jail-broken devices are detected and blocked by your MDM solution

Jail-broken iOS devices pose a serious security risk to the enterprise, as users may inadvertently introduce malware through the use of unauthorized apps. MDM solutions are able to detect jail-broken devices by running a series of checks and attempting to perform actions that are forbidden by Apple. If detected, the device can be blocked or granted restricted access.

Experts advise a multi-layered approach to jail-breaking, including educating users of the risks incurred by jail-breaking, as many are simply unaware of the implications.

Colligo Briefcase Enterprise has been designed for compatibility with all of the leading MDM solutions.

"We tested several iPad apps for SharePoint for their security features. Colligo Briefcase Enterprise was the hands-down winner"

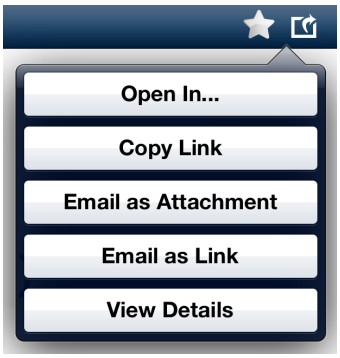
Markus Bosch, Solution Architect, Novartis International

NOVARTIS

5: How can I prevent sensitive corporate data from being shared externally?

Administrators can restrict users from emailing, printing and opening other applications

Using Colligo Administrator, sharing sensitive corporate data with external recipients can be tightly controlled. The administrator can disable the ability to email documents as attachments or print documents. Administrators can also restrict the set of applications that content can be opened in. This can be specified for a user or group of users. These settings can be disabled on an item-by-item basis.



Email documents as links for extra security

Colligo Briefcase Enterprise offers the option to email documents as links to SharePoint. This adds extra security, since the recipient must have the required SharePoint credentials in order to access the link.

Ernst & Young: Recommended Security Measures

High-Level Evaluation

- Third party apps to be reviewed for compliance with corporate security standards prior to deployment.
- Follow a secure application development process and adhere to secure coding guidelines.
- Ask vendors for enterprise versions of apps with central configuration and remote wipe functions.
- Ask an independent provider, such as Ernst & Young, to review the application.

Specific Security Implementation Recommendations

- Enable device protection using strong passwords.
- Encrypt SharePoint user credentials in the Keychain with an appropriate protection class, or avoid storing user credentials altogether.
- Encrypt storage of documents by iOS device encryption, or additional encryption if required.
- Enforce a password on app startup.
- Securely hash the app startup password
- Detect altering of configuration (.plist) files.
- Enforce protected communication to SharePoint (VPN, SSL).
- Harden the SharePoint site and backend.
- Use web application firewalls or entry servers.

Reprinted with permission from Ernst & Young joint webinar with Colligo 'The iPad Invasion - Leveraging SharePoint for Mobile Enterprise Security Feb 2012'.

"The use of tablets with SharePoint is a powerful combination, bringing improved productivity, availability and flexibility for business professionals; however, it is crucial that security risks are acknowledged and addressed prior to enterprise adoption."

Matthias Bandemer, Senior Manager, Advisory Services. Ernst & Young

ERNST & YOUNG

Colligo Briefcase Enterprise in Your Organization

Colligo Briefcase Enterprise free 30-day evaluation, request your copy now: www.colligobriefcase.com

For organizations that do not require the additional security, deployment, and management features in Colligo Briefcase Enterprise, Colligo Briefcase Pro is available from the Apple App Store. Organizations in selected countries can also purchase in quantity using Apple's B2B Volume Purchase Program.

Colligo Networks

Suite 400 - 1152 Mainland St.,
Vancouver, BC Canada
V6B 4X2

t 1.866.685.7962
f 1.604.685.7969
www.colligo.com