The iPad Invasion:

Leveraging SharePoint for Mobile Enterprise Security

With:

Matthias Bandemer, *Ernst & Young*

Barry Jinks, *Colligo Networks*

Trevor Dyck, *Colligo Networks*

Colligo Networks

Today's Agenda

- Speaker Introductions
- Impact and issues for iPads and mobile devices in the enterprise (Barry Jinks)
- Enterprise security issues for iPads and mobile devices (Matthias Bandemer)
- Using SharePoint and Colligo Briefcase for secure data access (Trevor Dyck)
- Q/A Session
- Next Steps

Our Speakers

Matthias Bandemer,
Senior Manager, Advisory Services

Ernst & Young
Quality In Everything We Do

Barry Jinks,
Founder and CEO

Colligo Networks

Trevor Dyck
Director, Product Management

Colligo Networks

Colligo Networks

Guest Speaker

Barry Jinks,
Founder and CEO

Colligo Networks

About Colligo Networks

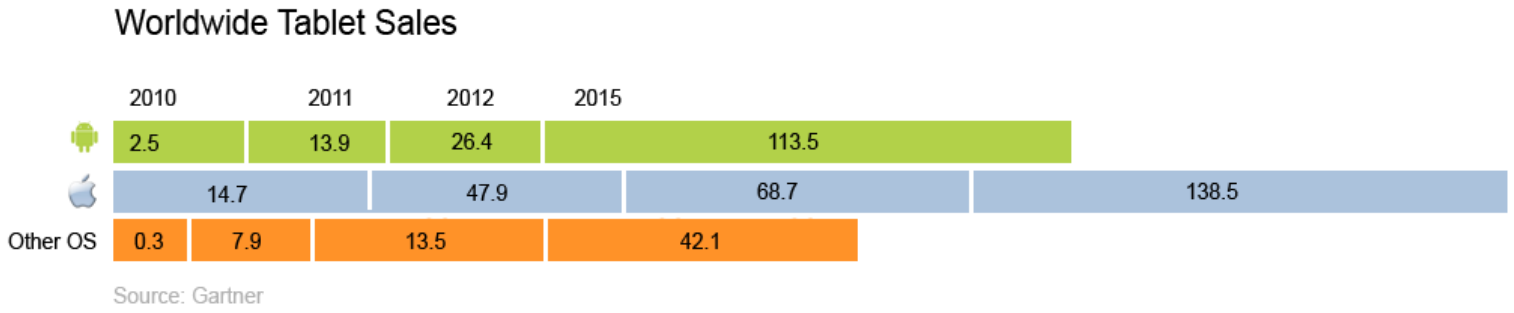
- Founded in 2000
- Focused on Enterprise Content & Records Management in SharePoint
- Award-winning pioneer and recognized leader in SharePoint apps that increase user adoption - “turning users into fans”
- Key partner (and vendor) to Microsoft
- Thousands of customers in 55 countries
- Multiple enterprise deployments in Global and Fortune 500

Select Customers

Colligo Networks

The iPad/Tablet Invasion

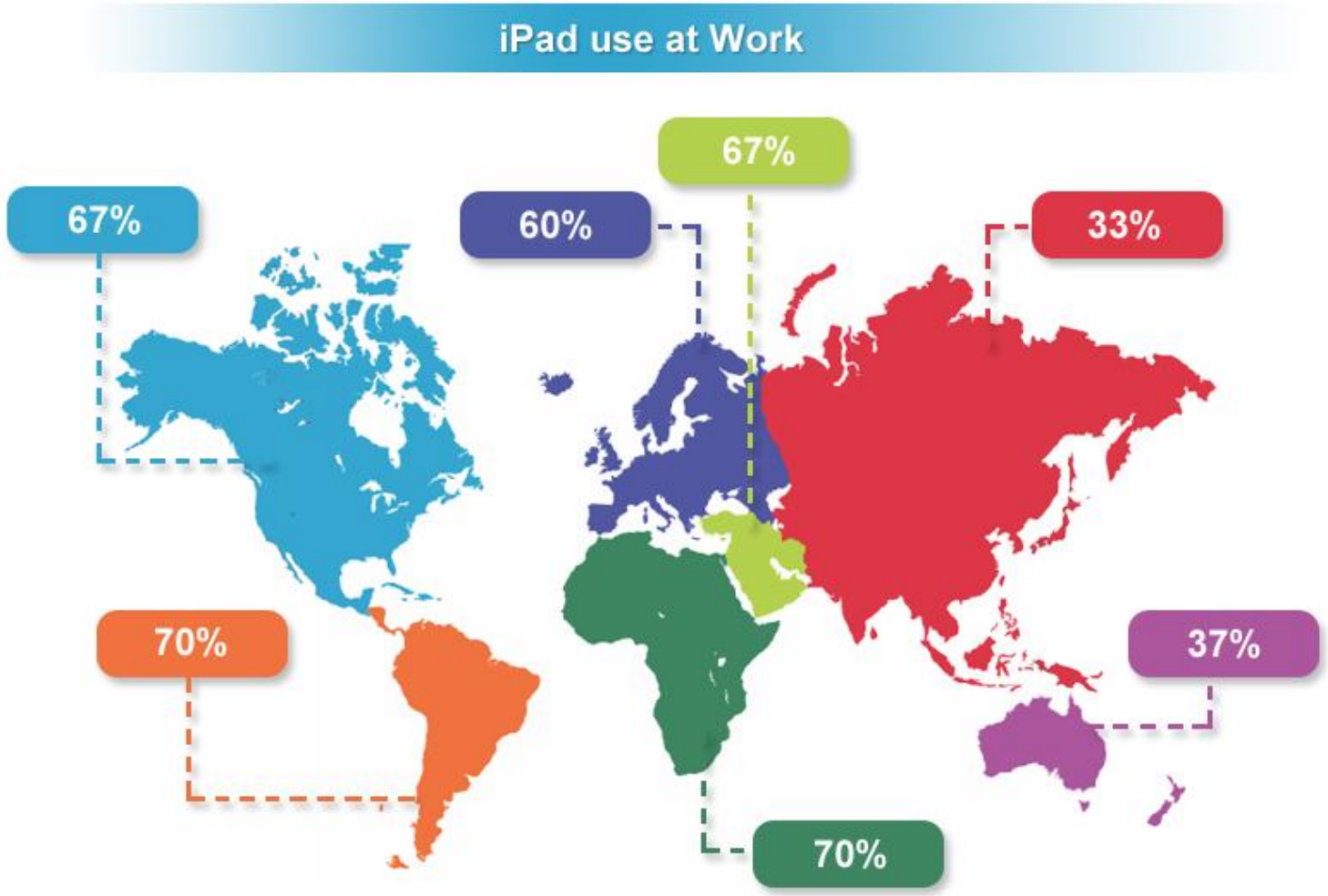
Source: Apple



Source: Gartner

Colligo Networks

Consumerization on the Rise

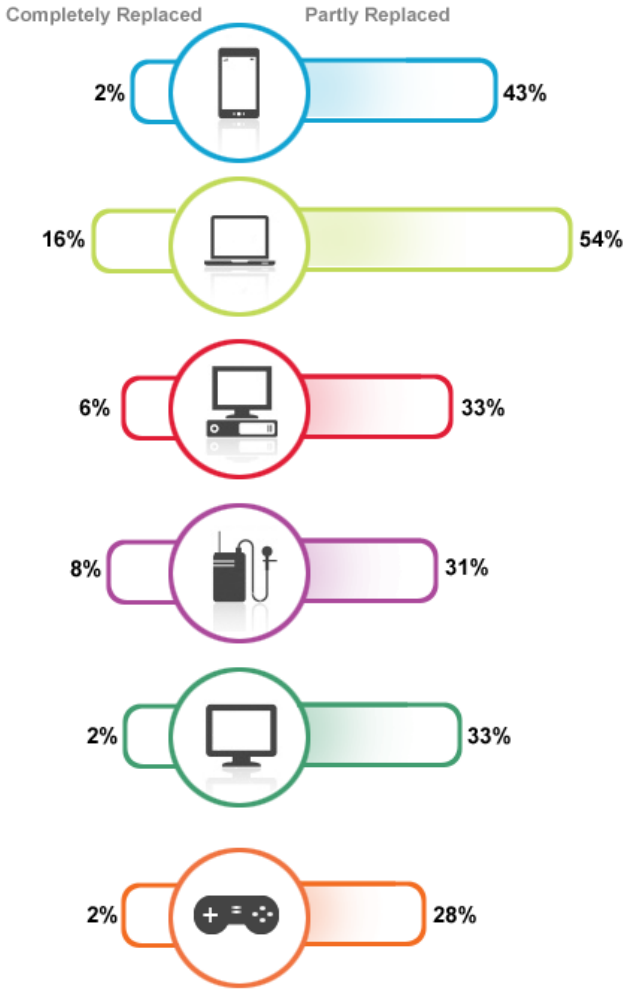


Professionals who use their iPad at work

IDC iPad for Business Survey 2012

Colligo Networks

iPad Replacing Rival Devices



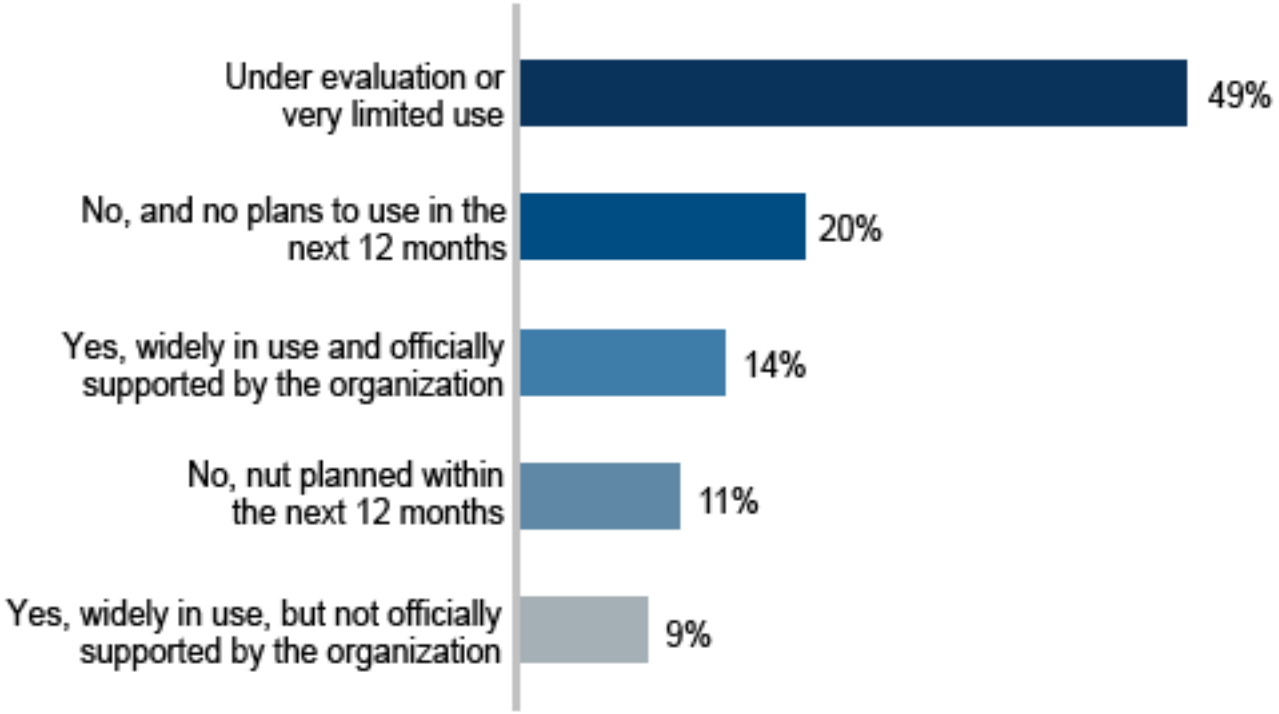
Number of professionals who say the iPad has partly or completely replaced the above devices

IDC iPad for Business Survey 2012

Colligo Networks

IT Support for Tablet Devices

Does your organization currently permit the use of tablet computers for business use?



Shown: percentage of respondents

Ernst & Young's 2011 Global Information Security Survey

Colligo Networks

Challenges for iPad in the Enterprise

June 20, 2011

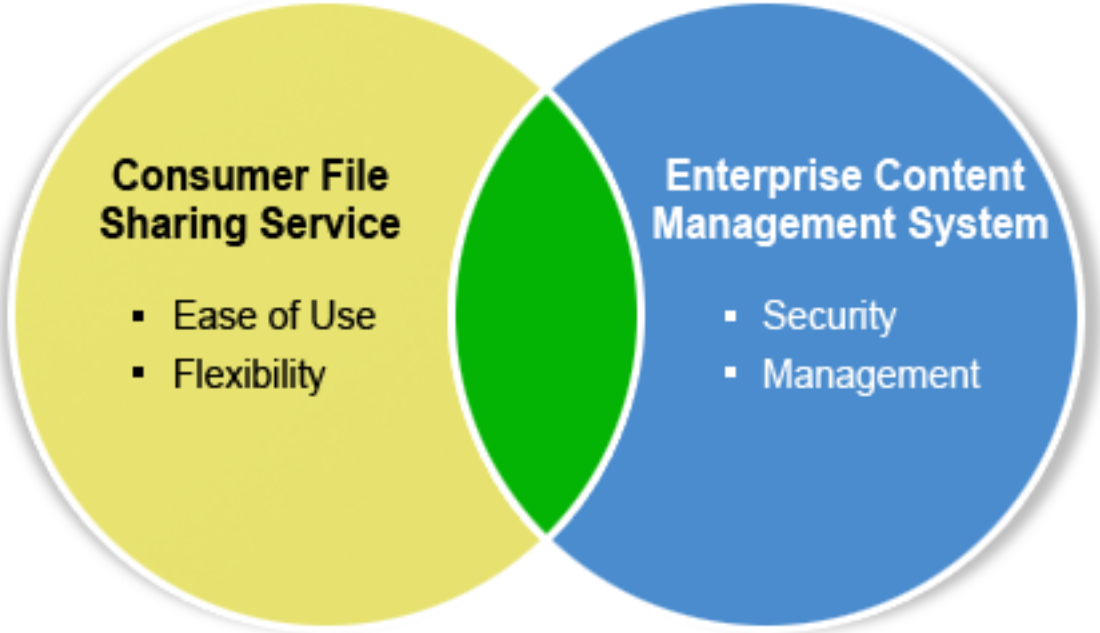
Dropbox Left User Accounts Unlocked for 4 Hours

At a time when hackers are on a tear looting information willy-nilly from insecure sites on the Web, Dropbox did the unthinkable Sunday — it allowed anyone in the world to access any one of its 25 million customers' online storage lockers — simply by typing in any password.

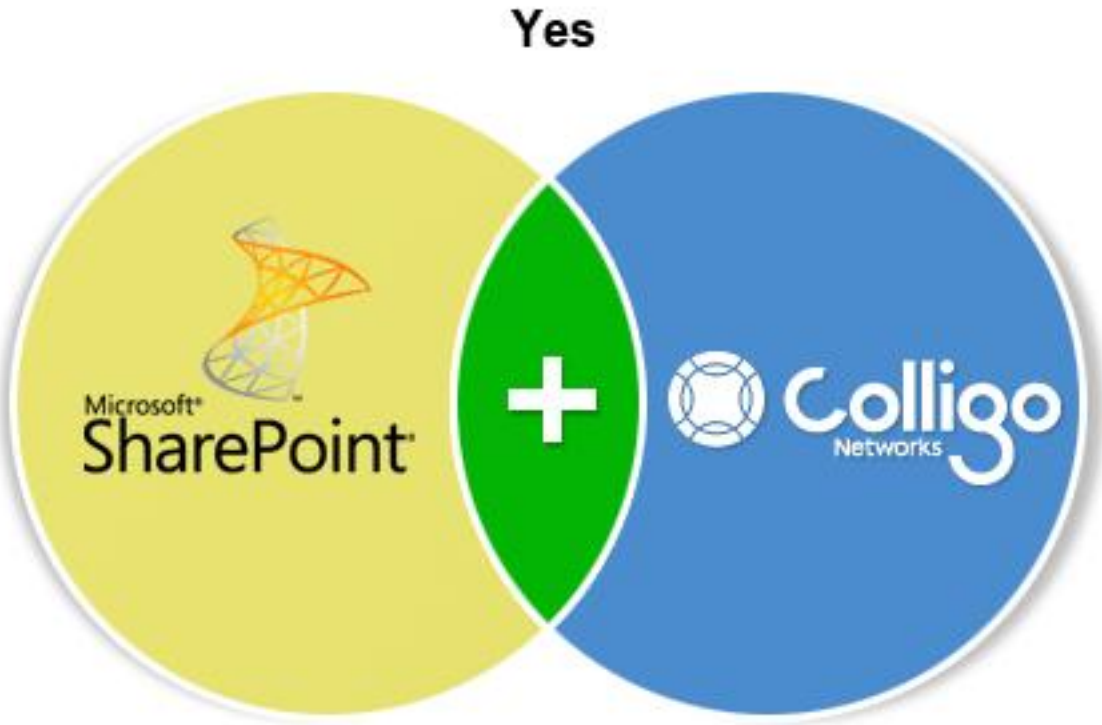
Dropbox, one of the most popular ways to share and sync files online, says the accounts became unlocked at 1:54pm Pacific time Sunday when a programming change introduced a bug. The company closed the hole a little less than 4 hours later.

Question

Is this possible?



Answer



Introducing Colligo Briefcase

The simplicity of iPad. The security of SharePoint.

Design Goals:

- Enterprise-grade security throughout
- A range of SharePoint features on the iPad
- Easy-to-use touch interface
- Caching for instant / offline access
- Compatibility with MDMs
- Sharing and management of content

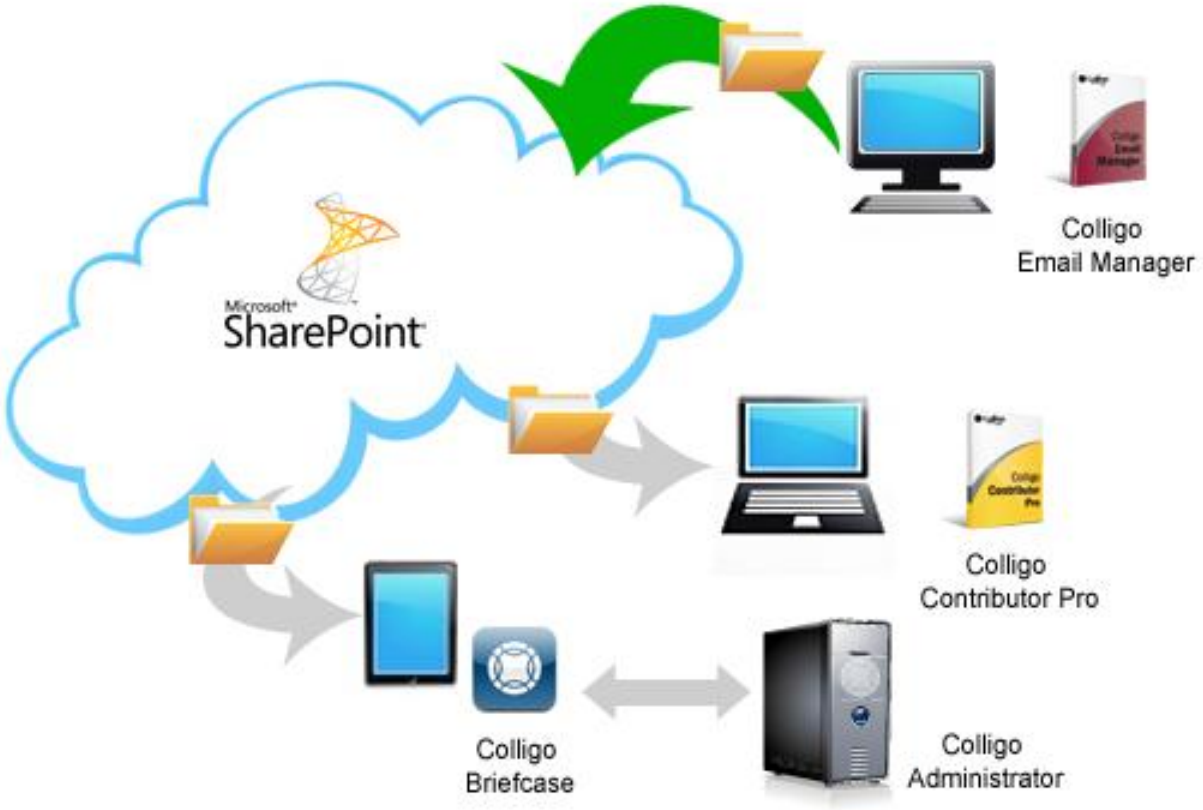
Colligo Networks

Content Sharing with Consumer Cloud Services

Dropbox, iCloud, etc.

- Security issues
- Management issues
- Control issues

Content Sharing with SharePoint + Colligo



SharePoint and Colligo

- Highly secure
- Centrally managed
- Easy file/folder sharing

Colligo Networks

Guest Speaker

Matthias Bandemer,

Senior Manager, Advisory Services

ERNST & YOUNG

Quality In Everything We Do

Colligo Networks

Introduction

- **Matthias Bandemer**
  Senior Manager at Ernst & Young Advisory Services
- 15 years of consulting experience in IT-Security, IT Risk Management, SOA and Cloud Computing
- Currently four iOS security experts in my local team based in Munich
- Global access to Advanced Security Centers

Ernst & Young has dedicated ASCs (Advanced Security Centers) with a global presence located in the Americas, EMEIA and Asia Pacific. Our Frankfurt and Dublin based ASC have invested heavily in a mobile device testing infrastructure that includes hardware devices and simulators.

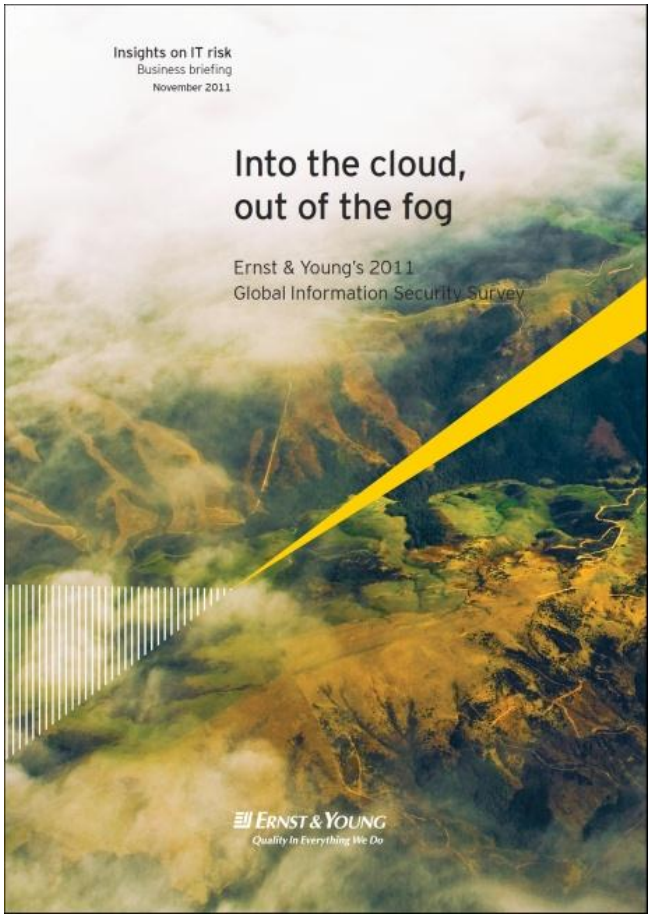
Enterprise challenges with mobile technology

The rapid adoption of tablet computing is evidenced by the results of our Global Information Security Survey.

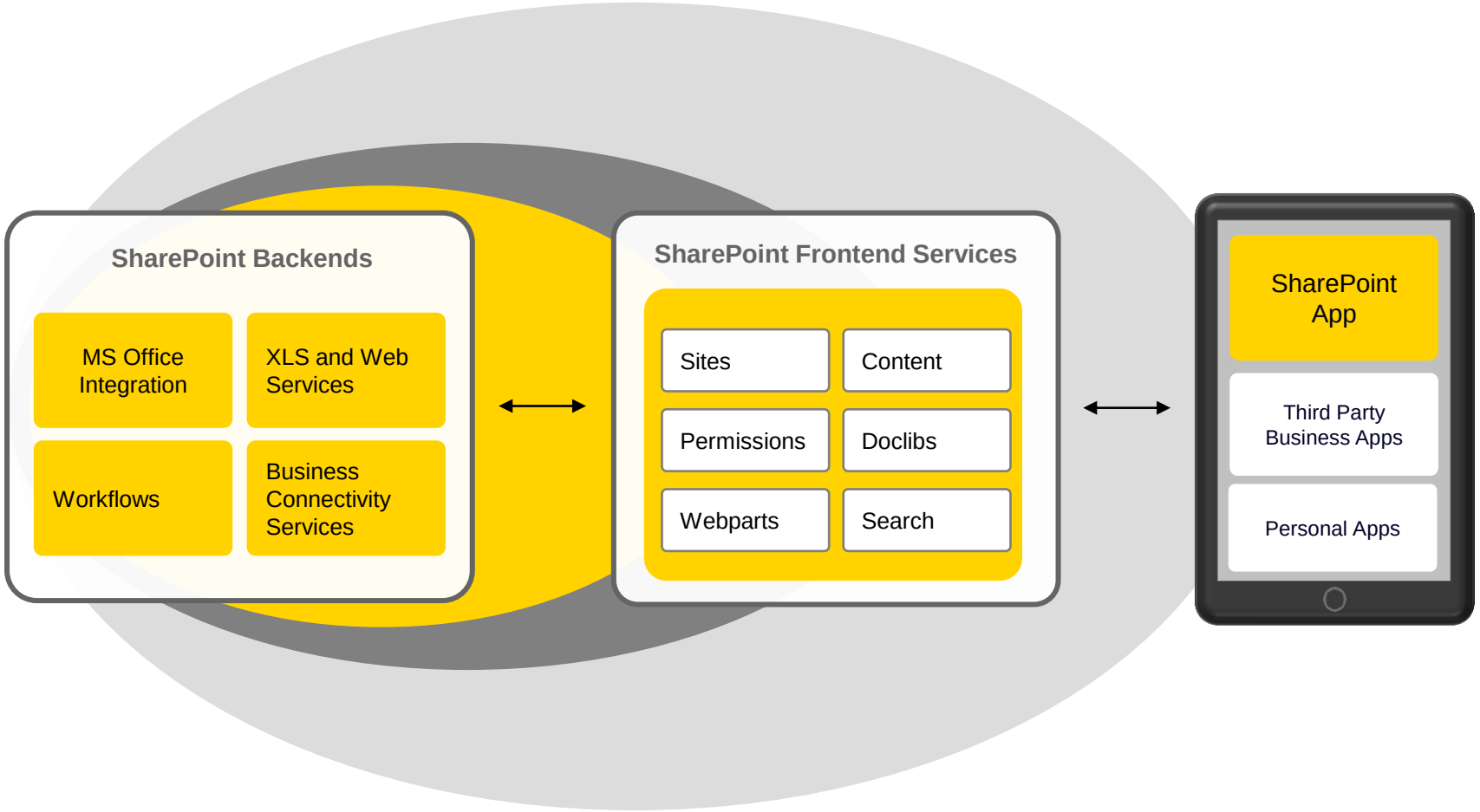
Only 20% of respondents do not have plans to permit the use of tablet computers; the vast majority of respondents (80%) are either planning to (11%), evaluating (46%) or widely using tablet computing (23%, of which 9% did not support use; 14% supported use).

On the other hand, our survey shows that the adoption of tablets and smartphones ranked second-highest on the list of technology challenges perceived as most significant, with more than half of respondents listing it as a difficult or very difficult challenge.

Source: Ernst & Young Global Information Security Survey, 2011



When the iPad meets SharePoint (1/2)



When the iPad meets SharePoint (2/2)

SharePoint

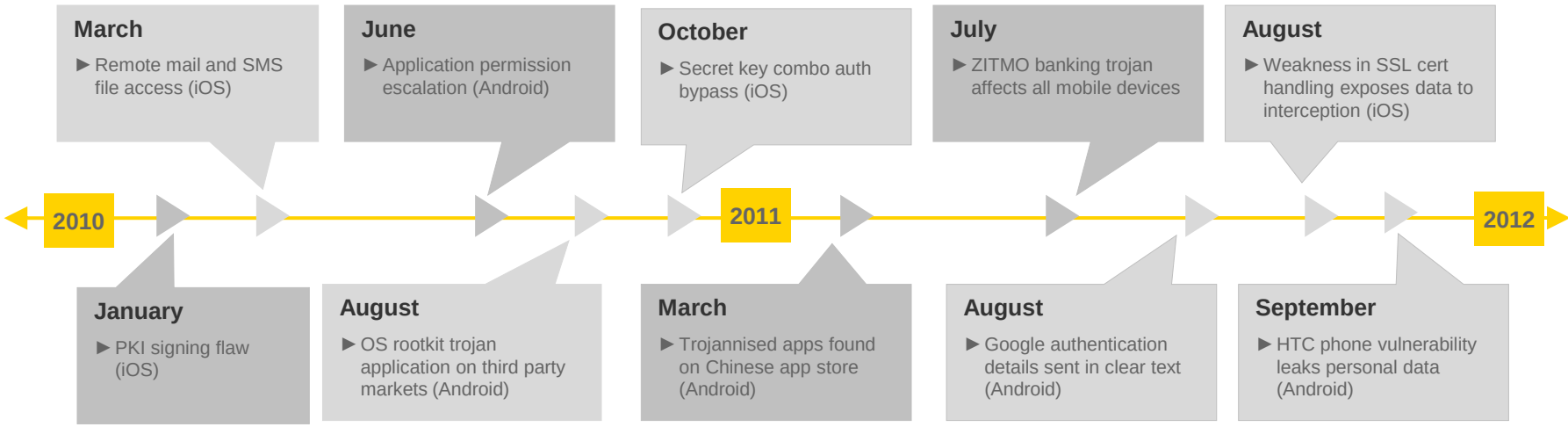
- A very popular infrastructure for collaboration, document management, enterprise content management, and workflows.
- Tight MS Office integration
- A comprehensive way of management of access to information
- SharePoint controls access to confidential information by access control.

Tablet computer

- Tablets like the iPad can be powerful SharePoint frontends regarding distributed team project management, tasks and schedules and mobile information collection.
- A dedicated SharePoint app can offer enhanced usability by optimized controls and views for tablet touch screens.
- Offline synchronization features allow mobile access to the entire office environment without network access

Our position is that tablet computers and SharePoint in combination can offer the opportunity for improved productivity, availability and flexibility for business professionals. Nevertheless, fundamental security risks must be acknowledged, evaluated and either accepted or mitigated prior to enterprise adoption.

Selected security weaknesses and vulnerabilities of mobile devices



Vulnerabilities and malware

- Many sandbox environments are not entirely secure. Rootkits and poorly secured application data mean sensitive information could be compromised.
- If data access controls are not configured correctly other applications could potentially access your application's data.
- Communications on wireless networks an ongoing concern
- Ongoing privacy issues with regard how platforms are using users' data.
- Highly customised and sophisticated banking trojans and Man-in-The-Mobile (MiTM) attacks circumventing controls previously thought to be secure (e.g. SMS/two-factor authentication).

User-borne threats

- Users can heavily influence the level of security of their device. Enterprise management may not be feasible in all cases and is typically not possible when dealing with customers.
- Safeguards preventing malicious applications from being installed can be bypassed by users, most likely tricked via social engineering (e.g. Disregarding excessive application requirements at install time).
- More applications mean more passwords. Users may often choose the same password for all applications. Your application may be secure but other apps may not be and may leak passwords and PINs.

The year to come

- Hackers are just getting started: Underground hacker forum activity and our intelligence from global offices suggests 2012 will see a wave of new mobile targeted attacks.
- Ongoing focus on customised attack vectors for banking applications
- Pressures of supporting multiple devices and platforms will increase the difficulty in managing security.
- Cloud services will further blur the boundaries of your network and reduce your sphere of influence and control on your data.
- Users will be further targeted with blended social engineering techniques

A jailbreak for the iPad 2 is available now!

- SharePoint enabled tablet devices seem to be a very attractive target
  - SharePoint user credentials or certificates
  - Authentication cookies
  - Confidential documents
  - Information disclosure by the screenshot capture functionality of iOS
  - Confidential information in logfiles

Jailbreaks available		
IOS VERSION	IPAD 1	IPAD 2
4.3	yes	no
4.3.1	yes	no
4.3.2	yes	no
4.3.3	yes	yes
4.3.4	yes (tethered)	no
4.3.5	yes (tethered)	no
5.0	yes (tethered)	no
5.0.1	yes	**yes**

January 2012

The SharePoint credentials of a user are a very interesting target for an attacker because he may gain access to the entire enterprise network infrastructure. In most cases the SharePoint account is the same as the Active Directory account.

Selection of recommended security measures

- Enable device protection using strong passwords.
- Encrypted storage of user credentials for SharePoint in keychain with an appropriate protection class or even avoid storing user credentials.
- Encrypted storage of documents by iOS device encryption or additional encryption if required.
- Enforce app startup password.
- Secure hashing of App startup password
- Detect altering of configuration (.plist) files.
- Enforce protected communication to SharePoint (VPN, SSL).
- Hardening of the SharePoint site and backend.
- Use of web application firewalls or entry servers.

Any third party app should be reviewed for compliance with corporate security standards prior to deployment.

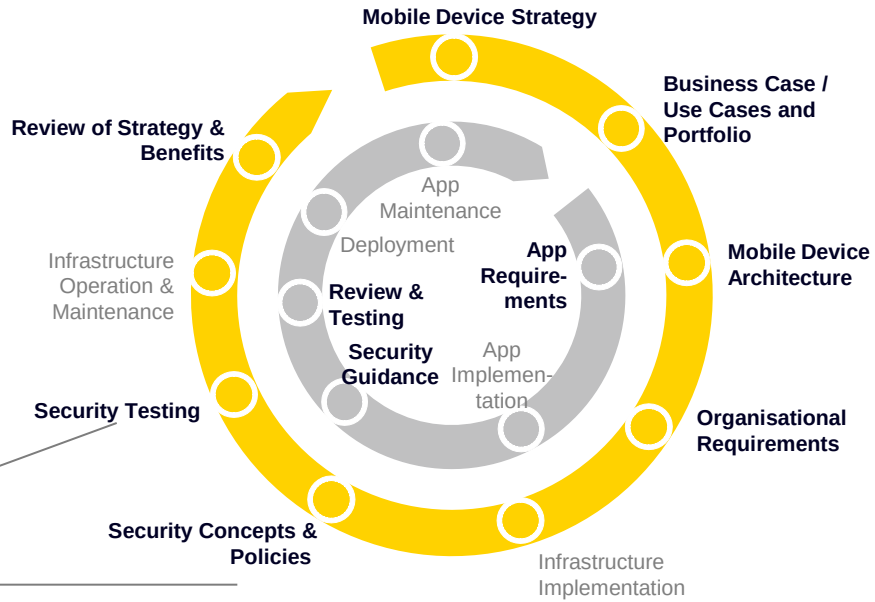
When developing apps follow a secure application development process and adhere to secure coding guidelines.

Ask vendors for enterprise versions of apps with central configuration and remote wipe functions.

Independent providers like Ernst & Young can do application or source code reviews or support the secure application development process.

How Ernst & Young can help.

Ernst & Young offers a wide range of information security and data protection services to assist organisations protect sensitive information (including credit card data, client data, personally identifiable information, intellectual property and trade positions). Beside, we demonstrate our understanding of the mobile technology lifecycle and highlight how Ernst & Young is positioned to support.



	Server Side application Testing (Web Service)	Application testing on Mobile device	Application testing on simulator
Black box	► SQL injection attacks ► Cross site scripting ► Session management ► Authentication ► Authorisation ► Information leakage ► Error handling ► Infrastructure testing	► Data storage / encryption ► File permissions ► Decompile application and review ► File system snapshots ► Wireless attacks ► Inadvertent caching ► Backup data analysis ► Jailbroken scenarios	► File monitoring ► Memory monitoring ► Process monitoring ► Network monitoring ► Debuggers ► OS version testing
Grey box	► All black box testing vectors ► Static code analysis utilising automated tools and manual review	► All black box testing vectors ► File monitoring ► Process monitoring ► Memory monitoring ► Network monitoring	► All black box testing vectors ► Application server configuration ► Device policy configuration ► Server infrastructure configuration

Bold = can be done / supported by Ernst & Young

Conclusion

The increasing mobile workforces are extending the enterprise, blurring the lines between home and office, co-worker and competitor and removing the traditional enterprise boundaries; resulting in access to sensitive data through Internet access, email accounts, and business applications like SharePoint.

An enterprise mobility management program should establish a framework to effectively manage the people, processes, and technologies that allow end users to access key data elements through mobile devices and secure apps.

Advisory Services

Olaf Riedel
Partner
Ernst & Young Hamburg
Telefon +49 40 36132 12415
Olaf.Riedel@de.ey.com

Matthias Bandemer
Senior Manager
Ernst & Young Munich
Telefon +49 89 14331 11976
Matthias.Bandemer@de.ey.com

Tobias Wahl
Senior Consultant
Ernst & Young Munich
Telefon +49 89 14331 15743
Tobias.Wahl@de.ey.com

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

Guest Speaker

Trevor Dyck

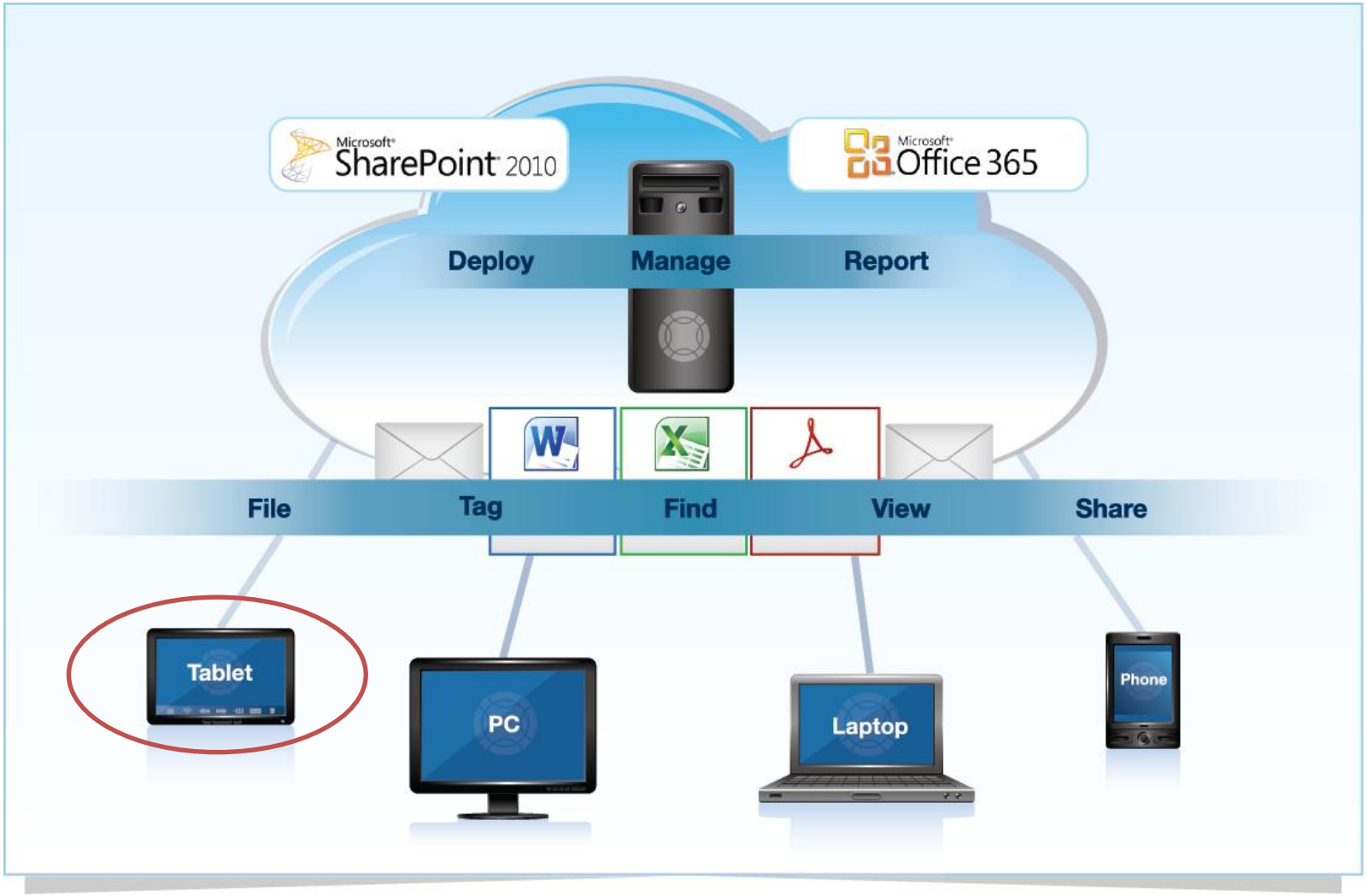
Director, Product Management

Colligo Networks

Today's Agenda

- Colligo for the Enterprise
- Colligo Briefcase
  - Security Features
  - Interface and Functionality
  - Integration with other Colligo products
  - Centralized management and administration

Built for the Enterprise



Colligo Briefcase

The simplicity of iPad. The security of SharePoint.

Secure mobile access to SharePoint content from the iPad

Colligo Networks

Intuitive Interface

- Extremely easy to use
- Intuitive menus and processes
- Utilizes standard iPad touch techniques, swipe, etc.
- Easily create Favorites for quick access

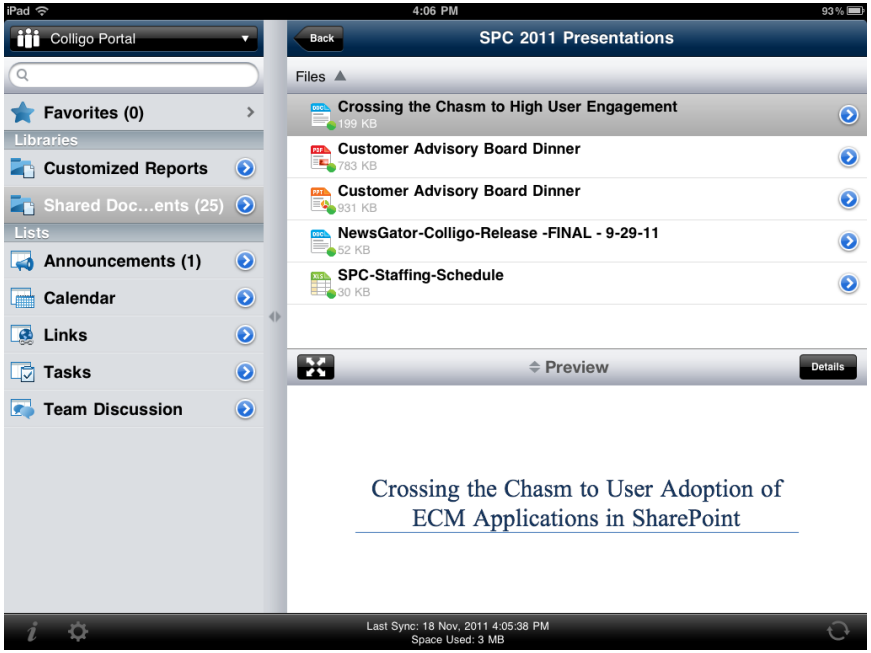
Colligo Networks

Enterprise Grade Security

- Separate passcode to access Colligo Briefcase
- Hardware-based encryption for all stored data (AES-256 bit)
- Supports all SharePoint authentication methods
- Remote data wipe capabilities
- Stored data can be wiped automatically on 10 failed login attempts
- SharePoint credentials stored in Keychain
- Ability to restrict the SharePoint sites accessed and content cached*
- Ability to restrict which content can be shared with external recipients*

* Via Colligo Administrator

Viewing SharePoint on iPad

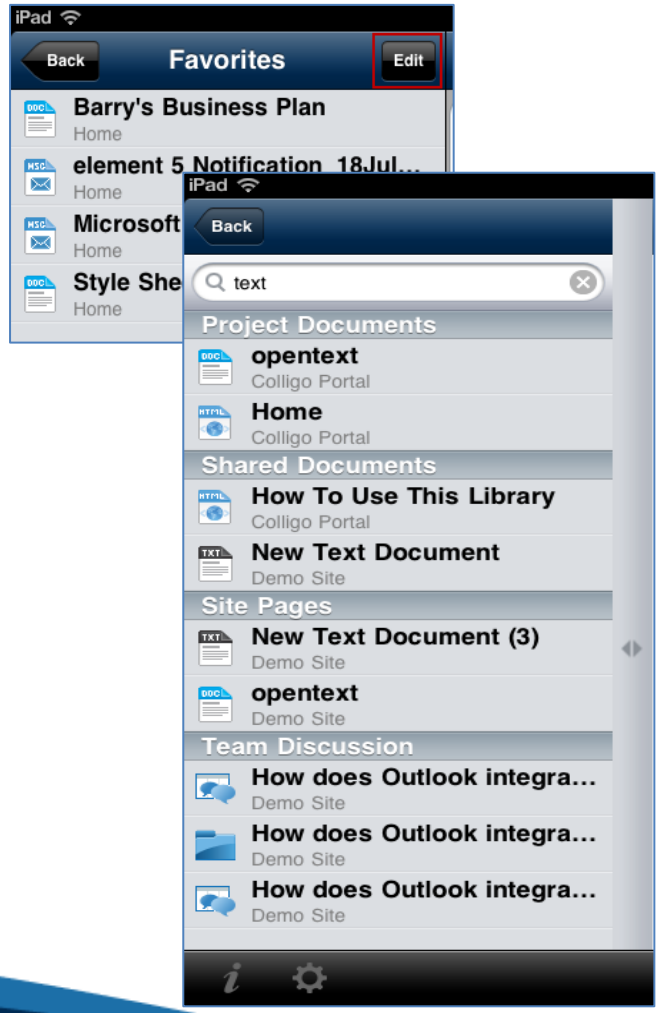


- Retains the integrity and context of documents and files
- View document properties including any metadata
- Easily preview files including .msg files (Outlook)
- Use SharePoint views to selectively display content
- Support for 23 file types

Flexible Cache and Sync Options

- Built on the industry's most tested and robust SharePoint sync engine
- Synch manually, on open, or specific intervals
- Synch specific items, libraries, lists or views
- Set limits to cache size
- Control syncing over 3G

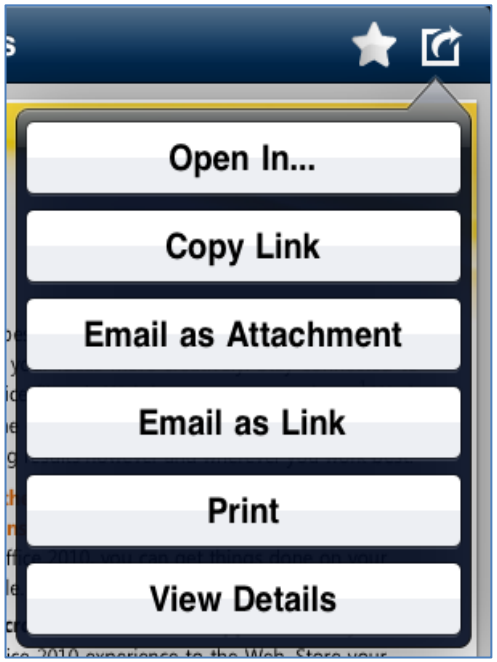
Easy Find and Search



- Search synced SharePoint content for documents and other files
- Set up favorites for quick access to commonly used folders and files

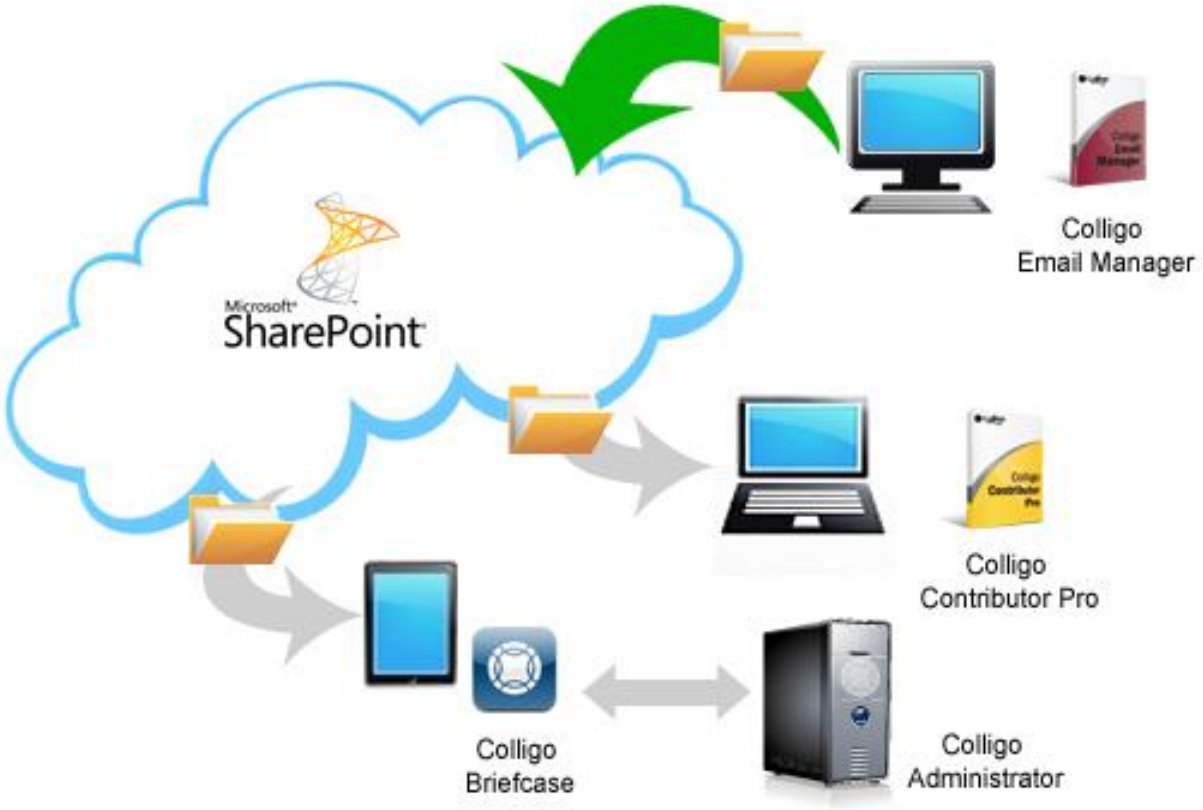
Colligo Networks

Actions on Documents and List Items



- A variety of item level options available to users
- Copy SharePoint link of item
- Email link increases security on items
- Specific options can be disabled via Colligo Administrator

Integration with other Colligo Apps



SharePoint and Colligo

- Highly secure
- Centrally managed
- Easy file/folder sharing

Colligo Administrator

Centralized configuration, management and reporting for Colligo applications

Deploy – Central provisioning for mobile and desktop devices, on-premise or in the cloud

Manage - Easily configure access to required content, without requiring IT

Report – Detailed metrics on SharePoint & Colligo usage

Colligo Networks

iPad Specific Management Capabilities

- Integration with MDM apps for automated deployment
- Centrally administer and push out the sites and document libraries that users/groups can access/cache
- Set several security-based configuration settings
- Restrict SharePoint sites accessed, content cached, and how content is shared externally
- Restrict options such as Print, Send as Attachment, and Open In
- Add/expire content
- Remote wipe of cached content

Colligo Briefcase Versions

Briefcase Lite	Briefcase Pro	Briefcase Enterprise
- Limited sync options and 50 MB cache	- Unlimited cache size	- Configuration via Colligo Administrator
- One SharePoint site	- Unlimited number of SharePoint sites	- Hardware based encryption
- Personal use only	- Support for all authentication methods	- Encrypted local data store with optional password protection
	- App specific passcode	- SharePoint credentials stored in Keychain
	- Support for Office 365/SharePoint Online	- Data wipe by admin or on 10 failed logins
- Free from App Store	- $14.99 from App Store	- Contact Colligo for details

Colligo Networks

Try Colligo Briefcase

Get Colligo Briefcase Pro »

Try Colligo Briefcase Enterprise »

www.colligo.com/briefcase

Available on the iPad
App Store

Colligo Networks

Summary

- Colligo Briefcase offers the first truly enterprise-grade SharePoint solution for the iPad
- Provides an easy way for organizations to utilize SharePoint to create a secure mobile enterprise data environment
- Addresses all the security concerns regarding mobile devices and enterprise data access/storage
- Provides centralized IT management and administration
- Integrates seamlessly with other Colligo SharePoint solutions for the enterprise

Q/A Session

Matthias Bandemer,
Senior Manager, Advisory Services

ERNST & YOUNG
Quality In Everything We Do

Barry Jinks,
Founder and CEO

Colligo Networks

Trevor Dyck
Director, Product Management

Colligo Networks

Colligo Networks

reviews@colligo.com

- Get Colligo Briefcase Pro
- Get Colligo Briefcase Lite
- Rate and write a short review of either product on the App Store
- Send your name, iTunes nickname and your email address to reviews@colligo.com

Available on the iPad
App Store

Colligo Networks

Next Steps

Get Colligo Briefcase Pro »

Try Colligo Briefcase Enterprise »

Access Webinar Recording on Resource Centre »

Contact Us: sales@colligo.com

www.colligo.com/briefcase

Matthias Bandemer,
Ernst & Young
matthias.bandemer@de.ey.com

Barry Jinks,
Colligo Networks
bjinks@colligo.com

Trevor Dyck
Colligo Networks
tdyck@colligo.com

Colligo Networks