Webinar: Mitigating the risks of uncontrolled content access from mobile devices

Presented By: Brian Ulmer, Product Management Director

Employees are going mobile

- Mobile devices are being used for an increasing number of day-to-day tasks
- Employees today expect to use these same, convenient tools to get their work done
  - 66% of users surveyed even take their smartphones to **lunch** in order to get work done*
- This is a great opportunity for productivity improvements

*Qualcomm survey 6/18/2013

2

Many enterprises are lagging

- Some enterprises are developing bring-your-own-device (BYOD) and mobility strategies

- Many have yet to institute formal policies

- 58% of businesses have **no BYOD policy** in place*

- 80% of businesses **have not trained employees** to understand BYOD privacy risks*

*Ponemon Institute - 2013

Acronis®

Bring-your-own-cloud (BYOC)

- Mobile devices do not include capabilities for secure access to most corporate content

- They also lack traditional central file management

- Users take it upon themselves to find a solution

- Free, public, consumer-oriented file syncing and sharing solutions are available and become the answer

The problem with BYOC

- Corporate content becomes spread between multiple, disparate solutions, introducing inefficiencies and disjointing workflows

- Sensitive files are moved into public cloud storage and can be shared with anyone

- Content cannot be audited or backed up

- Compliance requirements are not met

Acronis Mobility Overview

We provide anytime, anywhere content access, sync and share from any PC, Mac or mobile device, with the security and visibility and manageability required by enterprise IT

Control. Secure. Simple.

Over 8,000 Customers

Addressing Emerging Enterprise Needs

Enterprise Mobility	Secure access to enterprise file servers, SharePoint and NAS devices for mobile device users	mobilEcho™
Enterprise File Sharing	Secure syncing, sharing and collaboration on content	activEcho™
Apple in the Enterprise	Seamlessly integrates Macs in enterprise environments	ExtremeZ-IP®

What Today's Enterprise Users Want

Access, Share & Collaborate on Files with Different Constituents and on Multiple Devices

Access to corporate file resources on servers, NAS and SharePoint.

Sharing and collaborating on files with both internal and external people.

**Accessing and syncing files between devices – laptops, desktops, smart phones and tablets.**

Laptop   Desktop   Tablet   Smartphone

Comprehensive Secure File Access, Syncing and Sharing

Access to corporate file resources on servers, NAS and SharePoint.

Accessing and syncing files on user devices – laptops, desktops, smart phones and tablets.

Sharing and collaborating on files with both internal and external constituents.
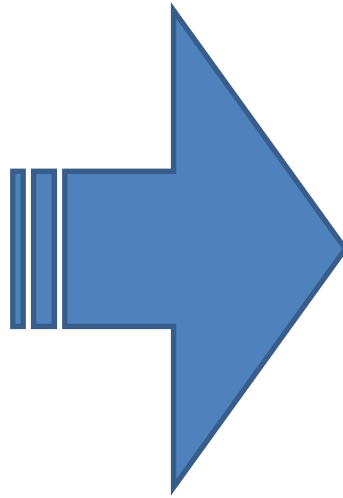
mobilEcho™

Secure access to enterprise file servers, SharePoint and NAS devices for mobile device users

activEcho™

Secure syncing, sharing and collaboration on files

Secure Mobile Access To Corporate Content

Requirement: Access to corporate content on servers, NAS and SharePoint.

mobilEcho™

Corporate Content

VPN, HTTPS Reverse Proxy or Firewall Route

Secure access to content on file servers, NAS and SharePoint.

Secure, embedded editing of Office documents, spreadsheets and presentations.

Policy engine for ease of management.

Active Directory integration - Support for certificate and Smart Card auth.

Key security features – encryption, remote wipe, etc

Simple, easy to use interface and navigation for end users

Securely Accessing Files Across All Devices

activEcho™

- ✅ Support for most popular mobile devices, desktop/laptops, browsers

- ✅ Secure, embedded editing of Office documents, spreadsheets and presentations on mobile device

- ✅ Policy engine for ease of management.

- ✅ Active Directory integration.

- ✅ Key security features – encryption, remote wipe, etc.

- ✅ Simple, easy to use interface and navigation for end users

Securely Sharing Files Inside And Outside Your Company

Requirement: Sharing files with internal and external constituents

activEcho™

- Management of authorized and unauthorized users

- Policy engine for ease of management

- Auditing

- Free basic sharing with external users

- Key security features – AD integration, encryption, remote wipe, etc.

- Simple, easy to use interface and navigation for end users

Acronis mobilEcho and activEcho: Driving Value with Common Technologies

Control
- Enterprise is in control - mobilEcho and activEcho run on-premise
- Single Management console to easily manage both solutions
- Acronis Policy Engine

Secure
- Active Directory integration
- In-App mobile Office editing and PDF annotation
- Audit logging
- Remote wipe of mobile devices
- Encryption

Simple
- Single mobile client
- Intuitive user interface and navigation
- Single, common server installer

Demo

mobilEcho 5.1 & activEcho 3.1

mobilEcho & activEcho Server Requirements

- Windows server platforms:
  - 2012, 2008 (inc. R2), 2003 (inc. R2)

- Windows workstation platforms:
  - Windows 8, 7, Vista

mobilEcho & activEcho Client Requirements

- activeEcho Desktop Client
  - Windows XP, Vista, 7, 8
  - Mac OS X 10.6 or later
- mobilEcho iOS Client Application Supported Devices:
  - iPad, iPad 2, iPad 3, iPad 4, iPad mini, iPad Air
  - iPhone 3GS, 4, 4S, 5, 5C, 5S
  - iPod Touch
- mobilEcho iOS Client Application Supported OS's:
  - iOS 5.0 or later
- mobilEcho Android Client
  - Supports smartphones and tablets
  - Android 2.2 or later

Questions??

Control. Secure. Simple.

www.acronis.com

www.grouplogic.com

www.acronis.com

@acronis