Achieving True Security in a Cloud-Hosted World

Introduction

After half a decade of working out the kinks on free, individual user accounts, major commercial cloud storage services such as Dropbox and Box recently set their sights on the corporate and small-to-medium business (SMB) paid-subscription market.

Those services have a compelling sales story to tell: Use our cloud to store and share your company's files, especially documents. Save yourself the hassle of managing the repository. Use our apps to make your files easily accessible to those who need to share them, on multiple supported devices. And trust us to keep them secure.

Attractive though that story may be to some organizations, it runs aground on two basic truths:

1. There are safer methods that make sharing even easier.

2. No matter how many ways providers assure customers that their files are safe, there's no escaping the inherent vulnerabilities in putting a third party in control of not only your document files, but also your encryption keys and log files.

This whitepaper examines the disadvantages of the commercial cloud model for document storage and sharing, and proposes a safer, more versatile model based on the combination of secure local storage and HTML5 document viewing technology.

Credibility and Cloud Services

Since rolling out to the corporate market, the commercial cloud storage services have had a rough time establishing a reputation for security.[i]

Although most commercial cloud storage vendors share the same vulnerabilities, Dropbox has emerged as the symbol of the problem, in part because it has experienced some very public security failures. The company has been linked to the PRISM scandal and the US National Security Agency (NSA) considered tapping Dropbox's servers as part of its controversial domestic surveillance program, according to press reports.[ii]

But for customer organizations, the main flaw in the commercial cloud model is that the service holds the encryption keys to customer files, not the customer. Although Dropbox and other providers tout their application of strong AES-256 encryption for customer files, the services hold the keys, and even permit selected employees to access and decrypt customer files.[iii]

4001 N. Riverside Dr. ▪ Tampa, FL 33603 ▪ P. 813.875.7575 ▪ F. 813.875.7705 accusoft.com

For its part, Dropbox admits that it routinely decrypts files, often without the customer's awareness, in order to make certain app features work, and that some of the metadata sent from mobile devices is transmitted without encryption.[iv]

Log files are similarly exposed on cloud storage services. Service employees can read, and potentially alter, records of customer activity. Both hackers and the government might also access this information, because it resides outside the customer's firewall, and out of the customer's control.

A practice called *file deduplication* opens yet another hole in Dropbox's security. When a file is uploaded, the service analyzes the file and compares it to files already stored by other users. If the file is identical to another, Dropbox writes a link to the previously uploaded file instead of storing the duplicate. Deduplication saves space and bandwidth for Dropbox, helping the company to keep prices down and profits up.

But security experts say deduplication can enable a third party to ferret out the contents of Dropbox's servers. For example, a law enforcement agency could upload a copy of a suspect file to Dropbox and measure the bandwidth consumed by the transfer in order to determine whether the upload was stored or a link was created to a duplicate file. This information could constitute probable cause to believe that a copy of the suspect file exists on Dropbox, enabling the agency to obtain a warrant for information about the duplicate's owner. [v]

Dropbox correctly argues that successful law enforcement requests are extremely rare, and that even with its inherent vulnerabilities Dropbox is safer than "not having current backups, not having any backups at all, accidentally deleting or overwriting files, losing USB drives with sensitive information, leaving files on the wrong computer, etc." according to the Dropbox website.[vi]

It's a reasonable pitch, but it really amounts to this: "We're not quite secure, but we're better than nothing."

One way or another, when an organization moves its files outside its firewall and entrusts them to a third-party service, that organization sacrifices some security. Companies make this sacrifice in order to provide convenient sharing and enable collaboration among employees. These companies are simply unaware that they can implement an even more efficient sharing environment while keeping their documents and their encryption keys safe on their own servers.

Keep Your Keys, and Share Away

A better solution can be found in a different way of thinking about document distribution and collaboration: An organization should have the ability to *show* documents without necessarily *sharing* them.

4001 N. Riverside Dr. ▪ Tampa, FL 33603 ▪ P. 813.875.7575 ▪ F. 813.875.7705 accusoft.com

In this all-important distinction, a new layer of document security is created, enabling organizations to meet user demands for information accessibility and collaboration while keeping document files, encryption keys and log files secure behind the organization's firewall and in the organization's exclusive control.

When document files are accessed from a cloud service, the actual document file is synced to the devices of authorized users, often in a file format that requires a native application for viewing, such as one of the Microsoft Office programs. Once open in the native application, the file can be modified.

Even if synced in "read-only" mode, the file can be saved under a new filename and manipulated, and content from the document can be selected, copied and pasted for use elsewhere. And whenever complete source files are synced, they run the risk of bringing malware along for the ride, to every device syncing the file.

Because of its high potential for unauthorized editing and misuse of document content, the commercial cloud storage model requires choosing between hiding the document from virtually everyone but those authorized to edit it (shutting out reviewers), or placing undo faith in the effectiveness of read-only mode as a security measure. This problem simply compounds the vulnerabilities caused by the cloud services' insistence on owning encryption keys.

Viewing Technology Shows without Sharing

HTML5 document viewing technology enables an organization to show a document without sharing it, all while keeping exclusive control of source files, encryption keys and logs. You have almost certainly used an HTML5 viewer, even if you may not have been aware of doing so. For example, the previewers for email attachments in cloud email systems like Yahoo! Mail are document viewers.

From the perspective of an end user of an HTML5 viewer, documents open in a browser tab or frame in which they can be read and also examined closely with such tools as zoom and text search. At the discretion of the publishing organization, the window may also include tools for annotating the document with comments, or redacting selected text or regions.

Behind the scenes, what's actually happening is that the original document, secure on the organization's server, is being very rapidly converted into a high-fidelity graphics file (such as the HTML5-standard SVG format) for transmission to the user's browser. The original, editable file never leaves the server, and never travels across the network or lands on the user's hard drive. The viewing file, though not the editable original, can still be encrypted in transit to protect its contents from unauthorized eyes.

4001 N. Riverside Dr. ▪ Tampa, FL 33603 ▪ P. 813.875.7575 ▪ F. 813.875.7705 accusoft.com

This technology can integrate seamlessly into a broad range of systems and environments. For example, HTML5 document viewing can be integrated with content management systems (CMSs) or with Microsoft SharePoint to serve as a default document display and collaboration window for managed files.

The security advantages of HTML5 document viewing over commercial cloud storage include:

- Document and image files, encryption keys and log files remain on the organization's server, behind the organization's firewall, in the organization's exclusive control.
- Mobile document viewing and collaboration requires only a mobile browser, not a third-party app. Source documents do not download to mobile devices, so bandwidth, plan minutes and on-board storage are not burdened by large, long file transfers.
- The end user never has possession of the actual document file in an editable form—although when appropriate, organizations can optionally add to the viewer a toolbar button that enables users to download the editable source document.
- Browser-based digital rights management (DRM) controls may be supplied by the viewer to enable the organization to disable text copying and printing.
- End users require no native application licenses in order to view, annotate or redact documents that may originate in many different file formats. This enables organizations to reduce the number of application licenses they purchase.
- The viewer may be customized, or put under programmatic control, to achieve such functions as automatic redaction of select types of content.
- Redacted documents can optionally be saved in fully formatted PDF files with all traces of the redacted text removed. Unredacted content can still be searched and indexed.

Conclusion

Many organizations are struggling to find a sweet spot that balances conflicting priorities of securing content, satisfying end-user access demands, and controlling infrastructure costs. Although commercial cloud storage does address all three issues, it fails on all three counts to deliver essential functionality and true security. For some companies, HTML5 document viewing technology offers a superior model in terms of flexibility, security effectiveness and cost.

Prizm Content Connect from Accusoft is an enterprise-class, server-based HTML5 viewer that supports hundreds of different file types through any HTML5 browser, desktop or mobile, and features tools for annotation, redaction and digital rights management (DRM). Visit Accusoft.com for more information.

4001 N. Riverside Dr. ▪ Tampa, FL 33603 ▪ P. 813.875.7575 ▪ F. 813.875.7705 accusoft.com

About Accusoft

Tampa-based Accusoft provides a full spectrum of document, content and imaging solutions as fully supported, enterprise-grade, best-in-class client-server applications, mobile apps, online and cloud services, and software development kits (SDKs). The company's Prizm Content Connect HTML5 document viewer supplies customizable, enterprise-class viewing, annotation and redaction for hundreds of file types. For more information, please visit www.accusoft.com.

---

[i] Marshall, Matt. "Dropbox has become 'problem child' of cloud security." *VB News* (http://venturebeat.com/2012/08/01/dropbox-has-become-problem-child-of-cloud-security), August 1, 2012.
[ii] Greenwald, Glenn and MacAskill, Ewan. "NSA Prism program taps in to user data of Apple, Google and others." *The Guardian*, June 6, 2013.
[iii] Singel, Ryan. "Dropbox Lied to Users About Data Security, Complaint to FTC Alleges." *WIRED*, May 13, 2011.
[iv] Acello, Richard. "App-solutely Perilous? Security of Mobile Apps Spurs Concern." ABA Journal, September 1, 2011.
[v] Schwartz, Mathew J. "Dropbox Accused Of Misleading Customers On Security." *InformationWeek*, May 16, 2011.
[vi] Drew; Arash. "Privacy, Security & Your Blog." The Dropbox Blog (https://blog.dropbox.com/2011/04/privacy-security-your-dropbox), April 21, 2011.

4001 N. Riverside Dr. ▪ Tampa, FL 33603 ▪ P. 813.875.7575 ▪ F. 813.875.7705 accusoft.com