Accellion Share Securely™

AN ACCELLION WHITE PAPER

Beyond Dropbox: Requirements for Enterprise Class Secure File Sharing and File Synchronization

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

WP-DB0112

Executive Summary

Consumer file sharing services are catching on with business users. But these services lack the rigorous security controls and centralized administrator of enterprise IT solutions.

Consumer services put enterprises at risk for data leaks, security attacks, and regulatory compliance violations. If a user transmits confidential information via untracked file sharing, the file transmission may constitute a regulatory violation that can result in financial penalties and a tarnished reputation for the organization.

This whitepaper explores the danger these “Dropbox” type services pose for enterprises, and the security and compliance requirements for deploying enterprise-wide file sharing solutions.

End Users: In Control, At Risk, and Out of Compliance

Consumer services put enterprises at risk for data leaks, security attacks, and regulatory compliance violations.

The temptation is understandable. A business user is working with multiple devices, such as a PC at the office, a Mac at home, a smartphone, and an iPad that travels between home and the office. She wants to share files across all these devices. She also wants to share files with co-workers and business partners, many of whom are working at remote locations. So she signs up for a free file sharing and file synchronization service such as Dropbox and selects which file folders will be shared. The service automatically copies her important files to all her devices and keeps them synchronized so they're always up-to-date. Co-workers and business partners are granted access to the files, as well. The service is fast, easy, and convenient.

It's also risky and potentially a violation of industry regulations and federal laws.

Consumer file sharing and folder synchronization services are catching on with business users. But these services lack the rigorous security controls and centralized administrator of enterprise class IT solutions. The consumer services put enterprises at risk for data leaks, security attacks, and regulatory compliance violations. If a user at a health insurance company transmits confidential patient health information, or a user at a brokerage transmits a stock recommendation, via untracked file sharing, the file transmission may constitute a regulatory violation that can result in financial penalties and a tarnished reputation for the organization.

The danger these "Dropbox" type services pose for enterprises is becoming increasingly apparent. One of the most popular consumer services, Dropbox, has been making headlines with its security shortcomings. Password protection was disabled for four hours, for example, and security researchers have discovered a way to make Dropbox accounts sync files with an unlimited number of devices that the account owner will never see.[1] IT administrators at businesses have no visibility into how employees are using these services. They have no way of determining how much confidential data their users are sharing improperly. Many IT administrators and compliance officers are frustrated, because they sense that a flood of data is leaving their enterprise networks, and they have no way of monitoring that flood or containing it.

[1] Derek Newton, "Dropbox authentication: insecure by design," http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/.

Devices and Files Everywhere

End users, meanwhile, remain imprudently enthusiastic. Millions of them are signing up for file synchronization services.[2] These services promise a hassle-free solution to many bothersome IT challenges. File synchronization is a 21st century solution to the plight of the 21st century mobile professional.

File synchronization is a 21st century solution to the plight of the 21st century mobile professional.

Users are juggling more devices than ever before. They have computers at work, computers at home, smartphones, and tablets. Through websites and web applications, they can access their personal data (email, social network feeds, blog posts) from any of these devices, and they'd like to be able to do the same with their professional data. The iPad that serves up video clips, weather reports, and family email on Saturday, ends up accessing business applications and business email on Monday. File synchronization makes this possible.

So does the architectural shift that's taking place in enterprise and consumer IT. The age of "fat clients" and PC-only applications is gone. Web services and mobile apps are the new platforms for business. To bring work data to personal devices, users are turning to cloud services, in the form of free, cloud-based apps. Users are inclined to trust cloud services, and are typically naïve about the security implications. Many of these services are free. Users can sign up for them with just a user name and a password. Users are already relying on these apps to share photos and music at home. Trusting them to manage files and folders at work seems like a natural progression.

Finally, as users work more frequently with video and graphics, files sizes are ballooning past the traditional 10 MB file-size limit imposed by email. Users need an easy way to share files of all sizes with colleagues. File synchronization, which users can configure in a browser with no official IT intervention, seems to be the answer.

But the security and compliance risks of these services are substantial. Let's take a closer look at the risks these services pose for enterprises.

[2] "Dropbox Hits 25 Million Users, Saves 200 Million Files Per Day," Michael Arrington, *TechCrunch*, http://techcrunch.com/2011/04/17/dropbox-hits-25-millions-users-200-million-files-per-day/.
[2] "YouSendIt Hits 30 Million Users, Bests Dropbox," Austin Carr, *Fast Company*, http://www.fastcompany.com/1755328/exclusive-yousendit-hits-30-million-users-bests-dropbox

Dropbox Security Exposures

April 2011—Security Researcher Discovers Dropbox Exploit for Hackers
In April 2011, security researcher Derek Newton discovered that Dropbox authentication relies on a single, unchanging hash code that identifies the computer being used to access Dropbox repositories. This vulnerability enables hackers to sync to a user's Dropbox files on any computer without being prompted for a user name or password. The owner of the Dropbox account will never know that files are being sync'd to an unauthorized device[3]

May 2011—FTC Complaint Alleges That Dropbox Can Read Files that Are Supposedly Encrypted
In May 2011, security researcher Christopher Soghoian filed a complaint with the Federal Trade Commission (FTC), alleging that Dropbox had been making false claims to customers about its protocols for securely storing data. According to Soghoian, Dropbox told customers that their files were encrypted and unreadable even to Dropbox employees, but his published research showed that Dropbox could read the content of any of these supposedly private encrypted files.[4]

June 2011—Password Protection Disabled
In June 2011, Dropbox accidentally turned off password authentication for millions of users during a software upgrade. For four long hours, every file in every Dropbox account could be accessed by anyone on the Internet without any authentication.[5]

Risks of Consumer File Sharing and File Synchronization

Consumer file sharing and file synchronization services pose these risks for IT security and compliance:

- **Data leakage**
  Users sharing confidential data with unauthorized users inside or outside the company can lead to data leaks resulting in fraud, loss of competitive advantage, and regulatory violations.
- **Loss of control over data access**
  Users sharing folders with other authorized users, in turn share folder access rights with unauthorized users. Administrators and even users themselves often have no idea who has access to files.
- **Security outages**
  Security glitches have the potential to expose confidential data to hackers and other unauthorized users. When a security glitch at Dropbox removed password protection from all user accounts, tens of thousands of files were accessed. Dropbox customers have no idea how many of those files were compromised.
- **Architectural weaknesses that create security vulnerabilities**
  Services optimized for personal use can have poor design decisions that create exploits that hackers can use to gain access to data; for example, folder names might be discoverable through brute-force attacks.
- **Compliance violations**
  Users sharing confidential data, such as financial records, outside the approved and monitored processes defined by the IT department, put the enterprise out of compliance with regulations such as SOX. Similarly, users at financial services institutions can violate GLBA by improperly sharing customer records. And users at healthcare organizations can violate HIPAA by improperly sharing patient health information.

[3] John Leyden, *The Register*, "Security researcher warns over Dropbox authentication security flaw," http://www.theregister.co.uk/2011/04/12/dropbox_security/. Also Derek Newton, "Dropbox authentication: insecure by design," http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/

[4] Christopher Soghoian, "How Dropbox sacrifices user privacy for cost savings," http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html

[5] Robert Dutt, *PCWorld*, "The Good, the Bad, and the Ugly of the Dropbox Authentication Error," http://www.pcworld.com/businesscenter/article/230804/the_good_the_bad_and_the_ugly_of_the_dropbox_authentication_error.html

Requirements for Enterprise Class File Sharing and File Synchronization

Enterprises need proven security features such as authentication, encryption, logging, and defense against brute-force attacks. IT administrators need to be able to control access to user accounts and individual files, so they can enforce company security policies and also keep a complete log of all file sharing activity in order to comply with industry regulations such as GLBA, HIPAA, and SOX.

Enterprise requirements for file sharing solutions include:

- **Secure workspaces for storing, syncing and sharing files**
  An enterprise file sharing solution should provide the convenience and automation of consumer services such as Dropbox, while also providing the rigorous security and compliance features that that enterprises need. Files and workspaces should be protected with password-based authentication. Files should be encrypted whether in transit or at rest. File repositories must be designed to resist attacks from hackers. Protections should be enforced 24/7, and users should always be able to determine who has access to files and folders.
- **Centralized administrative control over user accounts and files**
  Administrators should have control over all aspects of file sharing and access. Administrators should be able to control which files are shared and who has access to them. If an employee leaves the company, administrators should be able to shut off his or her access to files immediately.
- **Integration with existing directory and authentication services**
  The enterprise class solution should integrate with LDAP, Active Directory, SAML, and any other directory or authentication services that enterprises have in place to enforce access controls to data and IT services. IT organizations should not have to maintain a separate authentication infrastructure just for file sharing and folder synchronization services.
- **Integration with secure file transfer services (point-to-point, complementing the synchronization of files and folders)**
  Sometimes employees need to share files with external users or other users who do not have accounts with the file synchronization service. Rather than resorting to conventional email, which lacks robust security and tracking, employees should be able to switch to a secure file sharing service. This file sharing service should be integrated with the file synchronization service and make use of its account management, auditing, and encryption features, while supporting file sizes far beyond the 10 MB constraints of conventional email.
- **Rapid deployment; file synchronization service can be pushed out to all enterprise users**
  IT administrators should be able to deploy the new solution to every desktop with minimal manual effort. Deployment should be automated and centrally controlled.
- **Ability to block unsecure services such as Dropbox to enforce best practices**

To ensure the highest degree of security and compliance, enterprises should block the ports used by less secure services such as Dropbox. Blocking ports ensures that users who already have accounts with risky consumer services abandon those services and adopt the official, secure alternative.

- **Integration with Data Leak Protection (DLP) services**
  DLP services scan outbound communications to detect and block the unauthorized transmission of confidential data. File sharing and file synchronization services should integrate with (multiple layers of) DLP services an enterprise has already deployed, so that data security policies and industry regulations can be enforced consistently across the enterprise.
- **Monitoring, reporting, and auditing**
  IT organizations and security teams need to monitor file sharing activities to ensure that employees are adhering to company policies and industry regulations. For example, to comply with SOX, a business should be able to demonstrate that it is monitoring and controlling the flow of material financial data. IT administrators and compliance officers should be able to use dashboards, reporting, and audit logs to monitor the distribution of files such as financial reports, sales projections, and bank statements.
- **Flexible deployment options**
  Economics, agility, and scalability are leading more and more IT organizations to adopt cloud computing. The enterprise class services should offer a range of deployment options, including private cloud, public, and hybrid (combining on premise and cloud based services).
- **FIPS 140-2 certification**
  If the service is going to be used by government agencies, it should be certified as compliant with FIPS 140-2 to ensure that it enforces the rigorous security controls required by the federal government.

The table below summarizes the differences between a consumer class solution and a solution designed to meet enterprise requirements for security and manageability.

	Dropbox and other Consumer Services	Enterprise Solution
File Sharing and Folder Synchronization	Ad hoc and unmonitored	Secure, policy-based, and monitored
Risky File Sharing Services	Unmonitored	Blocked
Administrative Oversight	None	Dashboard, audit trail, tracking and reporting
Data Security Policies	Unenforced	Enforced
DLP Integration	None	Full integration
FIPS 140-2 Compliant	No	Yes
Security and Compliance Risks	High	Low

Conclusion

In an age of mobile devices and distributed teams, file sharing and file synchronization are essential IT capabilities. By deploying an enterprise file sharing and file synchronization solution, organizations can ensure that confidential data remains secure, while end users enjoy the convenience of accessing files from any authorized device, anywhere, anytime.

About Accellion

Accellion provides enterprise-class mobile file sharing solutions that enable secure anytime, anywhere access to information while ensuring enterprise security and compliance. The world's leading corporations and government agencies use Accellion to protect intellectual property, ensure compliance, improve business productivity and reduce IT costs. Founded in 1999, Accellion file sharing solutions can be deployed on public, private and hybrid cloud environments and provide the ease-of-use business users need while giving the enterprise organization the flexibility, scalability and protection it needs. For more information please visit www.accellion.com or call (650)-485-4300. Follow Accellion's Blog, Twitter, Facebook, and LinkedIn.