Dropbox Business

How Dropbox Business helps IT reduce risk

Legacy file sharing solutions were designed to keep internal data secure. They don't, however, provide safeguards for external sharing and user mobility — and this can introduce unexpected IT risk. With Dropbox Business, users are enabled to share internally and externally without compromising your ability to control and monitor the flow of data. Sharing controls, administrative capabilities, and activity monitoring help IT limit risk so that all of your teams can collaborate securely.

Email

Email is the most common method of sharing data externally. In a recent survey, Dropbox found that 88% of knowledge workers use email attachments to send files.[1]

Risks

Data control: Once an email attachment is sent out, data can be forwarded to anyone, making it hard to track who has accessed the file. It's also not possible to recall data once it's been sent over an attachment.

Version control: When documents are updated, a new file must be distributed, making it hard to keep track of versions and increasing the risk of data loss or leakage.

App usage: Email attachment size limits increase the risk that users will rely on alternative products to send larger files, which limits IT control.

How Dropbox can help

Sharing controls: Access to shared links or shared folders can be removed any time if you no longer want to share a document.

Audit logs: Sharing audit logs let admins monitor which users have shared which documents. Admins can also monitor views on shared links, including those sent to external parties, and external file requests.

Version control: Shared folders ensure that collaborators always have the most recent version of a file. Shared links update as documents are edited, so you can ensure that even external, view-only parties get access to the correct information. File requests let employees collect files from internal or external partners, where they'll automatically be organized into a Dropbox folder and stored safely.

App usage: Collaborators have convenient options for sharing files using shared folders and shared links, including right from their desktops or even Microsoft Office**.** Dropbox sharing is easy to use and has no file size limits, which keeps users on sanctioned products.

[1] Source: TNS-Dropbox Study, "Patterns of Collaboration," February, 2015

How Dropbox Business helps IT reduce risk

Continued

On-prem FTP

FTP helps avoid file size limits associated with email attachments. It's meant to increase security and control around sharing, but also carries its own risks.

Risks

Low adoption: FTP isn't the most user friendly solution and can be disruptive to workflows, which often results in low adoption. Frustrated users can fall back on unsanctioned solutions, reducing overall control and visibility.

Shared logins: Usage of the FTP requires employees to rely on IT for new accounts and does not support authentication methods like SSO. To save time, users share login credentials, which limits IT's ability to authorize and monitor access by user.

Limited visibility: It's not easy to understand exactly who is accessing the FTP server and what they are putting on it.

Strain on resources: Management of service and hardware requires greater IT resources. Without proper management, unpatched and zero-day exploits can open up a security vulnerability to the server and the broader network.

How Dropbox can help

Sharing controls: High adoption: With a highly usable interface that integrates into existing workflows, users readily adopt Dropbox Business. This gives you greater visibility and ownership of data.

One person, one login: Employees can create Dropbox Business accounts in seconds, which makes it much easier to regulate access on per-user basis. Sharing is easily targeted at the right people and can be monitored from the Admin Console, so it's easy to control who has access to what materials.

Simple management: There are no hardware management needs with Dropbox Business, and data is stored securely with multiple layers of protection. You can learn more about our security standards and policies at dropbox.com/business/trust.

Granular logging: The Dropbox Activity Feed provides visibility into who is accessing data and what they are doing with it.

How Dropbox Business helps IT reduce risk

Continued

USB Drives

USB drives are a familiar, user-friendly tool developed to support data mobility. However, they are difficult for IT to manage, and modern solutions can deliver greater security without compromising usability.

Risks

Lost hardware: USB drives can be physically lost, which increases the potential for data loss.

Vulnerability: USB drives can be subject to viruses and malware.

Limited visibility: USB drives don't allow for IT visibility into data access or sharing.

How Dropbox can help

Maintain usability: With Dropbox Business, you can keep the "drag and drop" interface that users love about sharing through USB drives.

No lost hardware: With Dropbox Business, you get the same mobility and easy sharing without relying on a physical device - and with deletion recovery and version history, no file is lost.

Increased visibility: While USB drives can be accessed anonymously, Dropbox Business records detailed logs of shared link access, providing admins with visibility into user activity and file sharing.

Protected devices: When employees link their devices to a Dropbox Business account, IT can protect information on these devices in the event that they are lost or stolen.