e-share

SOLUTION BRIEF

Is Secure File Sharing from the Cloud Really Impossible?

PROBLEM STATEMENT

Cloud file sharing and storage platforms such as Google Drive, Box, Dropbox and Microsoft OneDrive have enabled an easier and more cost-effective way of sharing information with internal teams and co-workers. But what about sharing private, confidential and regulatory-protected information with external parties such as legal teams, supply chain partners, third-party vendors and even customers?

Sure, these platforms do support external sharing. You can require the recipient to register for yet-another-account and hope that this is not too much friction for the collaboration you are initiating. And you'll have to hope that the file links you provided are not blocked by the recipient's firewalls or those of the country they reside in (e.g. China). The result is that users don't have the certainty that they expect of their cloud file sharing tools. Their emails always go through; why shouldn't their file sharing always work?

And given that cloud file storage providers can access the data you store, despite their BYOK encryption solutions, there are many who decide not to store highly sensitive data in cloud file storage. Data such as PII, non-public financials, and crown jewel trade secrets. What do you do when there is a need to securely share this data with external parties?

Simply put, you've got great solutions for internal sharing, but you're rolling the dice when you need to share information with external parties.

e-Share is the first and only external file sharing solution that utilizes your trusted branding, existing cloud file storage and familiar email-based workflows to make external information sharing easy, reliable and secure. With e-Share you continue to use Google Drive, Dropbox, Box and OneDrive for your internal sharing, but you now have the reliability, ease-of-use, and security needed to use that same cloud file storage for sharing highly sensitive data with outside parties.

The advantages of using e-Share coupled with your cloud file storage for external sharing are detailed below.

RELIABILITY ADVANTAGES

Links used by e-Share for file/folder sharing are not blocked by corporate and country firewalls.

Highly security-conscious businesses block external links to cloud file storage services such as Dropbox, Box, OneDrive and Google due to concerns about data loss through personal cloud file storage use and phishing attacks. A recent survey has confirmed this is widespread, with 47% of 200 respondents confirming that they block external cloud file storage links. The implication for businesses is that they cannot rely on traditional cloud file storage services to get business critical data to their partners, supply chain and other external parties.

And the blocking extends to entire countries, with China, Saudi Arabia, Syria, Iran, Tunisia, Vietnam, Burma, Cuba and Turkmenistan routinely filtering, if not outright blocking, cloud file storage services. China is the most problematic, as it represents a large manufacturing partner and growth market for most businesses. A large US-based fashion retailer recently turned to e-Share to move 1TB of media files out of China over an 8-hour period in support of its annual fashion show, after testing confirmed that OneDrive and Dropbox were being blocked by the "great firewall of China".

e-Share avoids this blocking by using a customer-owned domain (e.g. cloud.humana.com, as opposed to humana.dropbox.com) for all file links and access to our web portal. Though our system uses cloud file storage services, such as OneDrive, for physical file storage, this fact is entirely hidden as the e-Share system proxies all access to this storage.

Businesses need to see from their file/folder sharing services the same level of reliability that they experience with corporate email.which they never question. With e-Share, business users never have to worry…the recipients of shared files/folders will always be able to access the data shared with them.

TRUSTWORTHINESS ADVANTAGES

Even if cloud file storage links are accessible to recipients, many will question the trustworthiness of those links given that the domain and associated certificate used for those links belong to Box, Dropbox, Microsoft or Google. Not so with e-Share.

This is especially concerning when recipients are being asked to complete a form online or upload files back to the initiator of the collaboration. When it's the recipient's data involved, they are more likely to question whether the request for data is legitimate. With e-Share, which uses the domain and associated certificate of our customer, this is avoided. Additionally, the web portal accessed by internal users and external recipients and the emails sent by the e-Share system (e.g. notification of file being access or uploaded) use the branding (i.e. logos and colors) of the customer. In combination, this yields a high-level of trust on the part of the recipient that they are dealing with a collaboration system approved and managed by the party it claims to be.

EASE-OF USE ADVANTAGES

Recipients of files/folders shared through the e-Share system do not require an account to access the data shared with them.

The adoption of file/folder sharing services and secure email services has been greatly hampered by the requirement that users have an account on whatever system is used to share data with them. Recipients do not want to another password to forget and many are often prevented from using their corporate email address to login into systems their business does not directly provision.

The alternative is anonymous links, but businesses almost universally disable these for very good reasons; the most important being that the use of anonymous links cannot, as the name implies, be tracked and audited. The result is a stale-mate, with the data owner requiring a login that the recipient either cannot or will not provide.

Though the e-Share system supports username/passwords for use cases and data that require this, as well as one-time access codes, most of the sharing done through the e-Share system takes advantage of our login-free, SmartURL technology. SmartURLs are links that are unique to each recipient, allowing their access to and use of shared files/folders to be tracked and controlled. This provides businesses an additional degree of freedom in striking a balance between ease-of-use and security.

Initiators of file sharing via e-Share can do so through the most ubiquitous of collaboration tools – email.

While most business users instinctively look to email to initiate and conduct their collaborations with outside parties, cloud file storage services are primarily designed to be used via web portals. Though the web portals, which e-Share uses itself, is ideal for some users and necessary to manage shared files (e.g. expire links, change share settings), the lack of email support diminishes the productivity of most users.

With e-Share, file and folder sharing, including a wide range of sharing controls (e.g. view only, online editing, etc.) can be initiated by simply attaching a file to an email. Users get the best of both worlds – initiating their collaborations through their familiar email system and managing their collaborations, when needed, through a web portal.

Unlike cloud-file storage services, file/folder sharing through e-Share is natively bi-directional, enabling true collaboration.

With e-Share, all file/folder sharing can optionally create a bi-directional virtual data room through which the recipient can share files back to the initiator, with notifications to the data room owner that a file is awaiting them. And all of this is done with no IT involvement, no provisioning of a recipient account…the virtual data room is created automatically. Though cloud file storage services are about sharing a file, e-Share is enabling true collaboration, with an emphasis on ad hoc, on-demand data exchanges.

SECURITY ADVANTAGES

Unlike Box, Dropbox, Microsoft and Google, e-Share's encryption system prevents e-Share, and the underlying cloud file storage provider, from accessing any/all unencrypted data that is shared through the e-Share platform.

While cloud file storage services natively offer encryption that allows you to bring-your-own-key, this key only protects you when you decide to sever your business relationship and render your stored data inaccessible. But while the relationship is active your cloud file storage provider has access to your key, and thus access to your data.

If a cloud file storage provider were served with a gag-order subpoena from a Federal or State Court to turn over stored files, the cloud storage provider would be able to and required to satisfy the information request…and the gag order would prevent them from telling you. However, e-Share's patented encryption system prevents us, and the cloud file storage vendor we are configured to work with, from fulfilling such a request.

Though the security controls provided by cloud storage providers may be sufficient for some businesses, they are not sufficient for all. e-Share is alone in meeting the needs of those who require the highest level of assurance that their data cannot be accessed by their cloud storage provider.

SUMMARY

The e-Share platform allows businesses to address the inherent limitations in their cloud file storage solution when used for securing and sharing sensitive data with external parties. The result is a higher level of adoption and satisfaction on the part of users, less risk of data loss or misuse for the organization, more trust on the part of external parties and an improved ability to meet compliance requirements for the protection of regulated data.