druva

Tip Sheet

5 Unseen Risks in Enterprise File Sharing

When it comes to file sync and share, two critical features to look for in a solution are ease of use for end users and enterprise-grade security. However, evaluating solutions based on only those two aspects does not guarantee that a solution will adequately meet enterprise needs. To avoid putting your corporate data at risk, here are five unseen risks that must be considered when evaluating file sharing solutions.

Risk 1: Data loss

The majority of each user's data ends up outside their sync folder.

The traditional model for file sharing is to provide a folder for end users to store data they want to share across their devices, the organization or externally. But a large percentage of user data is never placed within this specialized folder. In fact, research shows that the majority of each user's data ends up outside their sync folder, causing challenges if IT relies on file sharing services to avoid user data loss.

The way to avoid this risk is to use a solution that integrates continuous backup with file sharing, therefore performing a full backup of data across all devices. This takes the burden off the end user to place files in a sync folder, and gives IT the visibility and control they need as the protectors of enterprise data. Of course, if a backup solution is intrusive to end users, they will disable it. So it's vital that your full backup is enforceable by IT, is non-disruptive to end users, and will auto-resume if interrupted.

Risk 2: Exposure of private data

When cloud service providers hold encryption keys, they have the ability to decrypt customer data.

Enterprise file sync and share solutions generally tout encryption as a must-have feature. However, as many of these services hold the encryption keys themselves, they still have the ability to decrypt customer data, if they are legally required by subpoena or if impacted by rogue employees within the service provider's organization.

To assure corporate customers that their data is private, cloud service providers may escrow keys by placing the key in a third party provider's system that does not belong to the storage provider. When data is requested, the key is retrieved and the data is decrypted, but the key never remains with the storage provider. While this does provide some reassurances rogue employees cannot access customer data, data can still be handed over by subpoena or government inquiry.

A reliable way to ensure privacy is to use a two-factor encryption scheme, wherein the customer and third-party provider each hold a portion of the encryption key, preventing data from being decrypted without customer credentials. Using two-factor encryption, if a cloud service provider is subpoenaed, they will not be able to provide decrypted customer data.

Risk 3: Being out of compliance

File sharing solutions should supplement audit trails and policies with a file classification system.

To enable organizations to remain compliant, some file sharing solutions include audit trails to let stakeholders see how, when, and where data is being accessed, shared, stored, and deleted. Administrators typically have the ability to set policies to enable or disable different privileges – such as external sharing – at a user, file, or folder level.

However, these features only provide visibility and control within the specific file sync and share environment. To provide a comprehensive answer to compliance needs, file sharing solutions should supplement audit trails and policies with a file classification system whereby each file carries with it an identifiable tag that dictates its usage. This approach enables permissions to be enforced for a file no matter where it resides, even if it's outside the file sharing environment.

IT can further bolster compliance by ensuring a solution provides secure links – hyperlinks that are restricted so they can only be opened by the recipient – and domain blacklists and whitelists, which allow administrators to approve or block specific domains from receiving files.

Risk 4: Inability to conduct eDiscovery

Most file sharing solutions lack centralized visibility or workflows to place legal holds and collect data.

There is no straightforward, effective way to apply a legal hold when employees are using file sharing solutions, as file sharing solutions lack centralized visibility or workflows to place legal holds and collect data. Instead, IT ends up suspending users' accounts, then copying the data out of the file sharing service to intermediary storage. This solution is manually intensive, disrupts employee productivity and only provides current, not past, data. Furthermore, when file sharing services used by

employees lack audit trails, there's no way to be certain when files were created, modified or shared.

A solution that is built with governance and eDiscovery needs in mind will automatically capture data off all devices and back it up to a centralized server, while also providing administrators with built-in functionality to suspend retention policies, place legal holds, and export data for eDiscovery. A solution like this will guarantee that earlier versions of files or those that have been deleted can also be gathered for eDiscovery purposes, not just what's currently available.

Risk 5: Data breach

File sharing should have remote wipe and geolocation integrated for laptops and mobile devices.

File sharing solutions have no way to protect files from breach when devices are lost or stolen, and with 32% of data breaches caused by lost devices, according to Forrester, proactively protecting against breach is essential for organizations. As the majority of breaches occur on laptops instead of smartphones or tablets, a holistic approach that protects data on all types of devices is essential.

For this reason, file sharing should have device encryption, remote wipe, and geolocation integrated from the ground up for laptops, smartphones, and tablets. And with a comprehensive solution, after a device has been remotely wiped, all of the data from the device can be restored – not just data the user chose to sync.

Summary

When evaluating file sync and share options, it's easy for enterprises to focus solely on requirements around end-user experience and enterprise-grade security without considering other critical needs. While user experience and security are essential for any solution, ensuring that a solution does not place enterprise data at risk or create headaches for IT around issues of compliance and governance is just as critical.

About Druva: Built on AWS, Druva is the leader in converged data protection, bringing data-center class availability and governance to the mobile and distributed enterprise. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations on over 3 million devices. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.