ESG Brief

Commvault: Integrating Enterprise File Sync and Share Capabilities with Data Protection and Backup

Date: September 2015 **Author:** Terri McClure, Senior Analyst, and Leah Matuson, Research Analyst

Abstract: *Commvault recently added new enterprise file sync and share capabilities (EFSS) to its Endpoint Data Protection Solution Set. Commvault File Sharing will help end-users securely store, access, and share files from virtually anywhere, at any time, on any device. The EFSS capabilities address not only the burgeoning need for secure file sharing among business end-users so that sensitive data is protected, but also the critical need for organizations to more easily demonstrate compliance with regulatory and government requirements through further securing and protecting those files with an integrated endpoint backup solution. These new capabilities could give Commvault a competitive advantage in the file sharing and collaboration market, where most other offerings lack any means for secure collaboration in combination with an efficient endpoint data protection strategy.*

Overview

Earlier this year, Commvault announced new file sync and share capabilities, expanding the offerings within its Endpoint Data Protection Solution set. Commvault File Sharing offers the means to enable business users to safely store, access, and share files from virtually anywhere. The vendor is promoting its new file sync and share capabilities, which will provide an alternative, or complement, to existing solutions to ensure that sensitive and business-critical data will not only remain secure, but also in compliance with business and regulatory requirements.

Commvault also announced the availability of Edge Drive, a new feature available within Commvault File Sharing. Edge Drive offers users a virtual folder that acts as a "personal cloud" for real-time sharing across mobile devices, providing secure enterprise-wide access for file sharing and collaboration.

Commvault is offering prospective customers an opportunity to see first-hand how it can help them with the EFSS needs of their organizations. To that end, the vendor is giving away 30-day free trials to its Endpoint Data Protection solution. Those three trial levels include:

- Showcase Demo (Basic): Customers can view a showcase demo environment and the solution's features.
- End-user Capabilities (Intermediate): In addition to viewing the solution's features, customers can explore end-user capabilities. They can use Commvault's cloud vault to store their data, download a mobile app, or put an agent on their laptops.
- Administrator Capabilities (Top): By downloading a copy of the vendor's software onto their own servers, customers can investigate administration capabilities, as well as features and end-user capabilities—getting a total sense of the full solution.

Licensing

Commvault's customer feedback consistently indicated that organizations wanted different entry points and licensing options to meet their needs today—*not in the future*. To accommodate customer demand, Commvault offers user licensing in a number of iterations. The vendor now sells per-user licensing individually in the areas of endpoint, backup and recovery, and file sharing, and discovery capabilities can also be added. Additionally, the vendor offers one-, three-, and five-year term licenses, as well as perpetual licenses.

The Challenge of Securing and Managing Data While Meeting Compliance

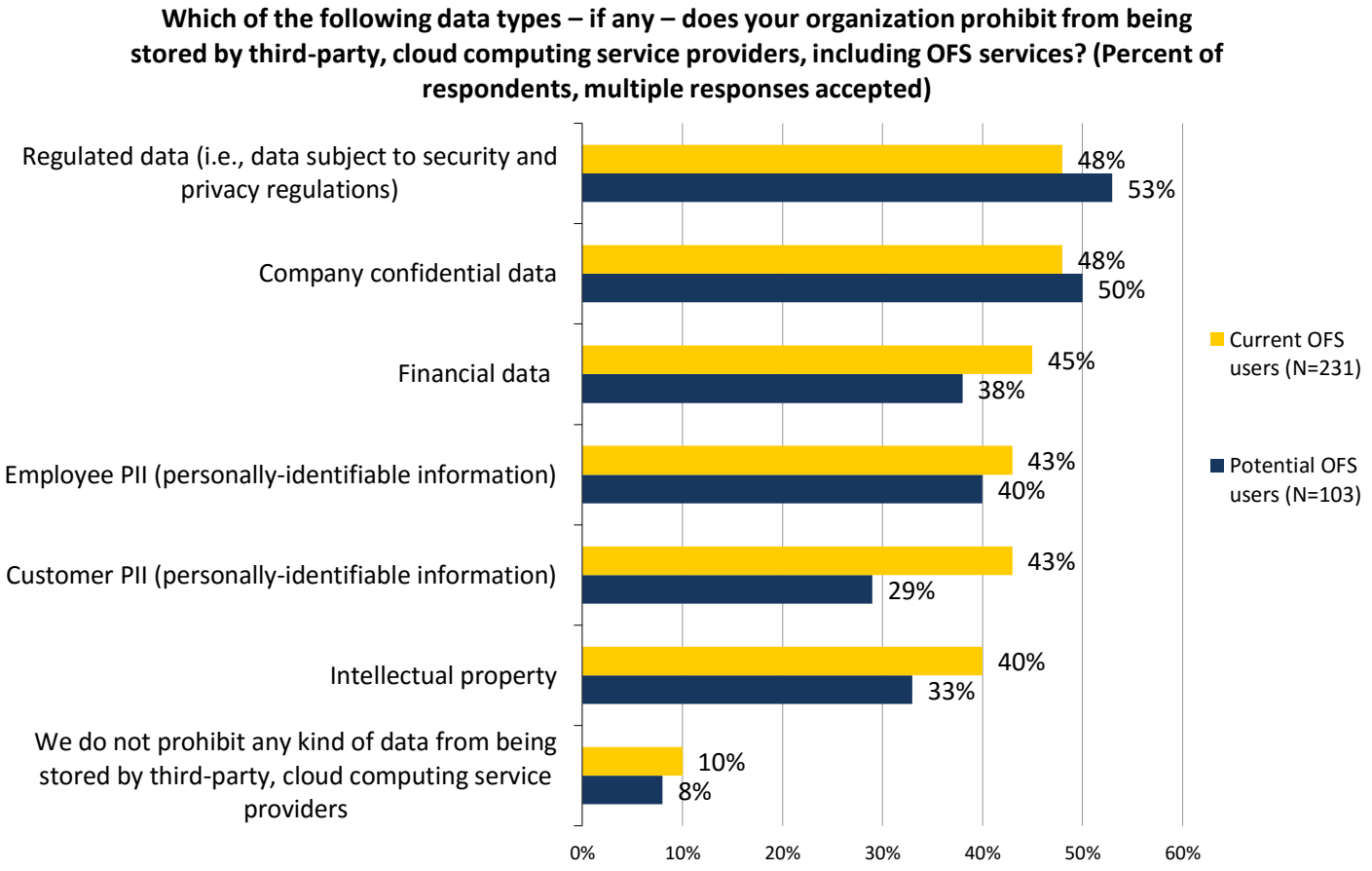
Today, business-critical data is facing increasing risk. With the growing adoption of bring-your-own-device (BYOD) policies, and business being transacted anytime, anywhere, on any device, many enterprises are confronted with

massive amounts of data that "lives" on a massive number of endpoints. More end-users are looking to access that data from multiple devices, sync it to their desktops and laptops, and share it with collaborators. At the same time, IT teams are focused on securing, backing up, managing, and appropriately retaining that data, while also trying to ensure that only the appropriate data is accessible to each employee. Those at the C-level are concerned with leveraging data to create new business opportunities, reduce decision making time, and speed business cycles, all while managing costs, reducing business risks, and reducing the organization's exposure to data breach. Security and compliance teams are trying to determine how they're going to cost-effectively perform discovery and search to meet compliance in addition to performing corporate governance. As if that weren't daunting enough, there's more.

When it comes to enterprise sync and share, many organizations have found themselves dealing with some serious solution sprawl. This often happens because, in order to make data searchable from multiple platforms and silos *while* maintaining compliance, organizations need to integrate third-party data protection, retention, search, and e-discovery tools. With a solution for this and a solution for that all residing on multiple platforms, businesses need a viable way to consolidate. Additionally, these same organizations find it difficult to trust a third-party vendor to securely handle business-critical and sensitive data.

Previous ESG research investigated the types of data that existing and potential EFSS users disallow from being stored with cloud service providers. The responses, which were mostly consistent across current and potential EFSS users, ranged from regulated data to intellectual property, but the bigger takeaway is that at least 90% of respondent organizations—regardless of current EFSS use status—report imposing restrictions on at least one type of potentially sensitive information (see Figure 1).[1] This seems to suggest that the majority of organizations have reservations around how service providers handle sensitive company data.

Figure 1. Types of Data Prohibited from Cloud Service Providers, Current versus Potential Users



Source: Enterprise Strategy Group, 2015.

[1] Source: ESG Research Report, *Online File Sharing and Collaboration: Deployment Model Trends*, February 2014.

Given this issue, it makes sense that 97% of organizations surveyed by ESG that have already deployed cloud-based EFSS solutions report that they are interested (and 69% said they are *extremely* interested) in a solution that would allow them to store some or all EFSS data on-premises.[2]

EFSS Is Not a Backup Replacement

While there are a number of EFSS solutions on the market today, most do not include a means of backing up files for protection, retention, and compliance purposes. No doubt, this is cause for concern—not only for IT, but also for CIOs and the compliance and risk officers charged with meeting compliance. Organizations must have control over enterprise data at all times, especially when it comes to business-critical and sensitive data, and most enterprises are not comfortable with storing that data in the cloud.

The backup issue is important and often overlooked. Many organizations are using EFSS as a backup replacement, but this could be putting data at risk. Approximately one-third of the current EFSS users surveyed by ESG and 42% of potential users report looking to achieve improved business continuance/disaster recovery by storing and/or backing up documents/files in the cloud with these solutions.[3] It is important to note that while EFSS has many of the same characteristics as data protection, such as the ability to recover old versions, it is not in and of itself a data protection solution. Yes, you can use these products to restore previous versions of files, and most allow end-users to restore accidentally deleted files themselves, which all sounds like backup. However, one rogue collaborator could delete an entire group's work, and his fellow collaborators may not notice until after the retention period has expired. As we continue down the path of using the EFSS system as the primary data store, with selective sync of documents to endpoint devices, is data truly protected? Not really—at that point, organizations have control over only a single copy of data, stored in the cloud, and have essentially abdicated backup and retention responsibility.

The purpose of EFSS offerings is collaboration and sharing, while backup protects and retains corporate data regardless of what device it is on. These are very different goals that require diverse governance and oversight. Backup requires set frequencies and policies to ensure compliance with corporate governance guidelines, while sync and share puts much of the retention and version control in the hands of employees who may not know governance policies. So organizations need both. If both can be accomplished through a single solution with overriding control for governance and protection, then all the better. That single solution would reduce the number of solutions procured and managed, and reduce data sprawl, thus mitigating the security challenges associated with having data in multiple places.

Commvault File Sharing: Collaboration, Consolidation, Compliance

For nearly 20 years, Commvault has been recognized for its backup and recovery solutions, helping organizations to decrease their risk exposure while lowering costs. In 2009, the vendor began offering deduplication and file view, adding scheduling and more source-side deduplication that covered not only Windows, but also Mac and Linux.

As the market began changing, the concept of workforce mobility was taking hold, and growing numbers of workers began conducting business remotely. Protecting data, while making it accessible, was essential. Customers wanted more than risk protection and backup; they wanted more usability and access to their data. Looking to answer the needs of the mobile workforce (and IT), Commvault continued to build on its efficiencies in backup and recovery by offering a means for secure and flexible data access, while also adding new features such as syncing across PCs, mobile apps, data loss prevention, and analytics.

Today, the vendor's Endpoint Data Protection Solution set encompasses endpoint data backup and recovery, security and data loss prevention (DLP), compliance and discovery, analytics and reporting, and file sync and share. Its DLP offerings help to reduce the risk of data breach, with tools that include geolocation, remote wipe, and bi-level encryption. Its analytics and reporting capabilities enable organizations to gain insight into file type, size, and age, among other details, enabling them to make informed decisions around that information.

[2] Ibid.
[3] Ibid.

And with its expansion into enterprise file sync and share (EFSS), Commvault now offers a viable means for IT to control data for sensitive use cases, giving IT visibility into the data, while also allowing users to securely share, collaborate, and be productive from virtually anywhere.

With its core backup and recovery business, Commvault is already securely collecting data held in a secure repository. Extending that functionality to EFSS offers a natural solution for those ongoing issues with which IT continues to struggle—namely, how to provide secure and flexible end-user collaboration, efficient solution consolidation, and an easy way to meet compliance. Commvault offers:

Secure File Sharing and Collaboration. Data is secure and available, giving end-users easy accessibility and flexibility anytime, anywhere, from any device (think laptops, PCs, smartphones, and tablets).

The Ability to Keep Data On-premises. Organizations don't have to pick and choose what data is eligible for the solution based on cloud policies—data remains on-premises and within the firewall, in full control of enterprise IT.

Efficient Consolidation. Organizations can now reduce the number of files being retained. This translates into saving time and resources by being able to optimize the infrastructure and the network, expending fewer resources since files no longer need to be sent over the network multiple times for multiple solutions.

An Easier Means of Compliance. With a user's data stored in a single repository accessible to any web browser or mobile device, most organizations—especially those in highly regulated industries such as healthcare and financial services—will now be able to more easily meet strict compliance, regulatory, and governance requirements.

Commvault File Sharing with Edge Drive offers the following:

- A single, fully integrated data repository where end-users can access files without giving up data ownership.
- Secure file sharing that provides flexible collaboration capabilities.
- Improved governance and compliance with enterprise search and discovery of on-premises data center and endpoint data, and legal hold capability.
- Administrative control, which allows for setting and managing policies and permissions.
- Enterprise-grade security, which means data is encrypted at source, in transit, and at rest.
- Increased security and usability to mobile devices, improved mobile productivity, and content syncing across devices.
- Seamless file/folder sharing from Edge Drive with others via the web or mobile app, with the ability to browse, download, manage, and restore files from the Edge Drive folder to local devices.
- Flexible deployment options including on-premises, hybrid, and cloud.

The Bigger Truth

Many companies today are in a constant struggle to find the most efficient, cost-effective solutions to enhance workforce productivity and meet the needs of a mobile workforce, *and* do so in a secure manner. While some EFSS vendors are stronger in delivering the flexibility that end-users want, others excel in delivering the control the business needs. Commvault appears to be focusing on delivering both.

Originally known as a data backup and recovery company, Commvault has ventured into the area of secure enterprise file sync and share. As a result of its roots in backup and recovery, Commvault is able to not only capture data, but also make it accessible for performing security encryption, analytics, discovery, and research. This means that organizations may no longer require a third-party solution to gain insight into what files sit in their repositories. This all can be accomplished using a single platform, streamlining the entire process, while making the solution more cost-effective. Companies dealing with the challenges of end-user-driven initiatives such as file sharing and collaboration should look into Commvault's Endpoint Data Protection solution set to consolidate their data backup and recovery solutions, while gaining insight into their data and performing compliance more easily.

Working closely with its customers appears to have given Commvault a good understanding of what its customers want and need: improved end-user productivity, and security and control for the business.

Commvault's EFSS capabilities not only address a burgeoning need for secure file sharing among business end-users, but also tackle the critical need for organizations to be able to demonstrate compliance with regulatory and government requirements. These capabilities could give Commvault a competitive advantage in the file sharing and collaboration market since most other solutions just offer a simple means for secure collaboration or an efficient way for enterprises to meet compliance—but not both. With the way the market is headed, Commvault appears to be well positioned with its technology. That said, in order for the solution to continue to be valuable to end-users and organizations alike, the vendor needs to continue to focus on enhancing its file sharing capabilities, growing its enterprise discovery capabilities, and being able to integrate more fully with data in the cloud.