ESG Lab Test Drive

Transporter from Connected Data

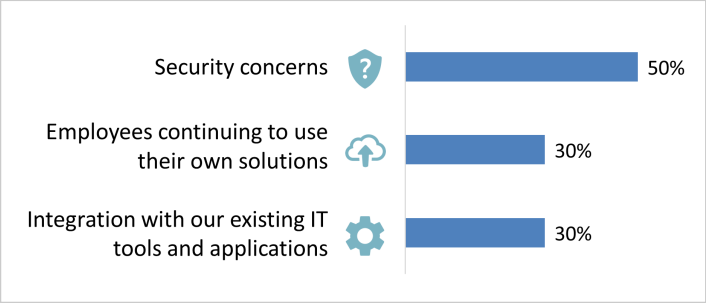
Date: February 2015 **Author:** Kerry Dolan, Lab Analyst and Vinny Choinski, Sr. Lab Analyst

Abstract: *This report documents the results of an ESG Lab Test Drive of the Transporter private file sync and share appliance from Connected Data.*

Challenges

Data at Risk

Online file sharing (OFS) solutions (also called "file sync and share") have become very popular for corporate as well as personal data. While NAS solutions have been the primary vehicle for corporate data sharing, products like Box and Dropbox are easier to set up, simple to use, provide access from any location or mobile device, and offer a certain amount of free storage. This is an appealing set of qualities, particular in a world in which the desktop PC is no longer the only computing platform. *Unfortunately, many employees leverage these public-cloud solutions for corporate data without the knowledge or permission of corporate IT departments*. As a result, petabytes of corporate data are at risk, residing in cloud solutions without the protection and monitoring of corporate IT, and often violating industry compliance or governance regulations—which can result in hefty fines. When ESG asked potential corporate OFS account adopters about their top concerns, their three most popular responses were security, employees continuing to use their own solutions, and integration with existing IT tools and applications. [1]



Lack of IT Control

Most organizations today want to bring control of their data back in house, but that is unlikely to happen unless they can provide their users a solution for storing data that includes the same levels of mobile device access, ease of use, and sync/share capabilities as public cloud OFS products. The genie is out of the bottle, and employees simply won't stop "going rogue" unless there is a solution that is better than standard NAS. Traditional file servers and NAS systems provide IT control, but remote access is limited to particular machines and often requires VPN access, which can add a level of complexity. In addition, once they access their data, they must navigate a shared drive system set up by IT, rather than their own directory structure.

Duplicate Data

Organizations are storing significant amounts of duplicate data in NAS systems, as they make copies of files for sharing, collaboration, and to use on other devices. This is driving up storage and management costs.

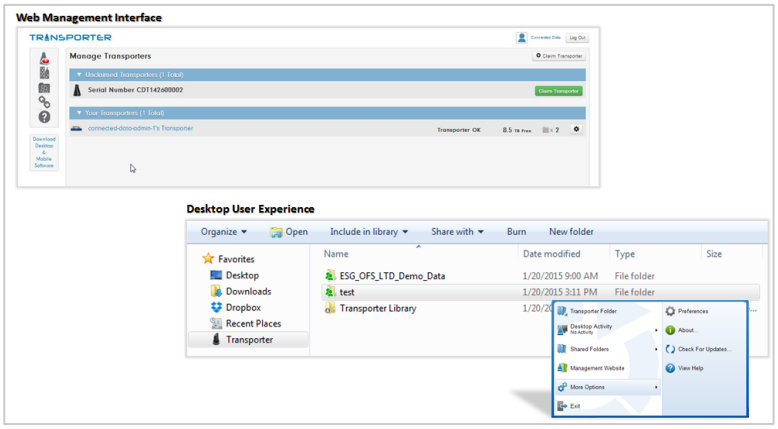
Data Protection and Security

Data protection and security are significant issues with public cloud solutions. Users generally have no idea where cloud providers actually store data and how they protect it. Corporate IT has no control over backup and recovery since this data is not within their backup schema. Should there be a cyber-attack on the cloud provider, the data is at risk. In addition, should the employee leave the company, IT has no idea what corporate data is stored online and cannot ensure that it is managed properly. Similarly, should an employee's laptop be lost or stolen, IT has no access to prevent a data leak into unknown hands.

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

Transporter from Connected Data

Transporter is a private-cloud, file sync and share appliance designed to provide the easy-to-use features of popular online file sharing (OFS) solutions, but with the IT control and visibility of traditional file servers and NAS systems. It is 100% private with encrypted transfers for security and helps businesses address compliance and regulatory requirements by giving corporate IT full control over the solution. Transporter enables IT to choose the location, synchronization, and redundancy of their file data. It can be easily integrated with existing infrastructure, and appliances can be added as needed in a grid-like fashion to sync offsite and scale. Organizations gain the benefits of cloud-based data that can be accessed from any device or location, synchronized, and shared easily, but with the privacy, protection, and security that they provide other corporate data.



Connected Data currently offers six (6) Transporter models that support up to 150 organization users per appliance:

- Transporter 150: packaged in a 2U, rack-mount chassis with ~20TB of usable storage and support for up to 150 organization users
- Transporter 75: packaged in a 2U, rack-mount chassis with ~10TB of usable storage and support for up to 75 organization users
- Transporter 30: packaged in a desktop chassis with ~9TB of usable storage and support for up to 30 organization users
- Transporter 15: packaged in a desktop chassis with ~6TB of usable storage and support for up to 15 organization users
- Transporter & Transporter Sync: small desktop devices designed for SOHO environments

The Transporter 150 and 75 solutions are targeted at the mid-range enterprise markets and integrate with smaller Transporter appliances for deployment flexibility. They deliver business-class architecture features such as redundant hardware, SSD metadata acceleration, single instancing per device, and automated, real-time syncing between authorized devices.

All business-class Transporter appliances integrate with Microsoft Active Directory, offer organizational administrator accounts and group management, and support advanced features such as file versioning, undelete, and read-only access. Transporters store data only on authorized devices that are managed by IT, eliminating any privacy concerns. Data is automatically synced to a cache on the client device, ensuring fast local access and multi-site redundancy.

Focused on a user-friendly experience, Transporter offers an extremely simple interface that integrates with native operating system explore and search capabilities (such as Windows Explorer and Macintosh Finder), and enables users to organize files as they see fit. It eliminates the need for complicated VPNs while still providing security via AES 256 encryption and data stored on company-owned infrastructure. Versioning, auditing, and read-only controls ensure data safety and conflict resolution.

ESG Lab Test Drive

ESG Lab tested a Transporter 75 from both the user and administrator perspectives. Transporter appliances are easy to set up and connect to networks, and can be claimed via network or through the MAC address. Once claimed, a Transporter will appear in an accessible list for use. The Lab created accounts for two users (VC and KD) and tested dummy accounts set up by Connected Data.

The User's Perspective: Desktop Clients

Transporter offers two user account types: organization users and guest users.

- Organization users can create folders and invite other users to share files; they are also responsible for setting access permissions. Organization users cannot manage Transporters or other organization users.
- Guest users have access only to files and folders that they have been invited to share. They cannot create shared folders or invite other users to share. Organization users set access permissions (read-write or read-only) for guest users.

All users have their own desktop folders in which files are automatically synced and shared between both organization and guest users. Administrators define which Transporters each user can access, and when users want to access files the Transporter application will automatically detect the most local device for use. For example, if the user has access to Transporters at the corporate headquarters and a branch office, when that user visits each location he will automatically be connected to the local device.

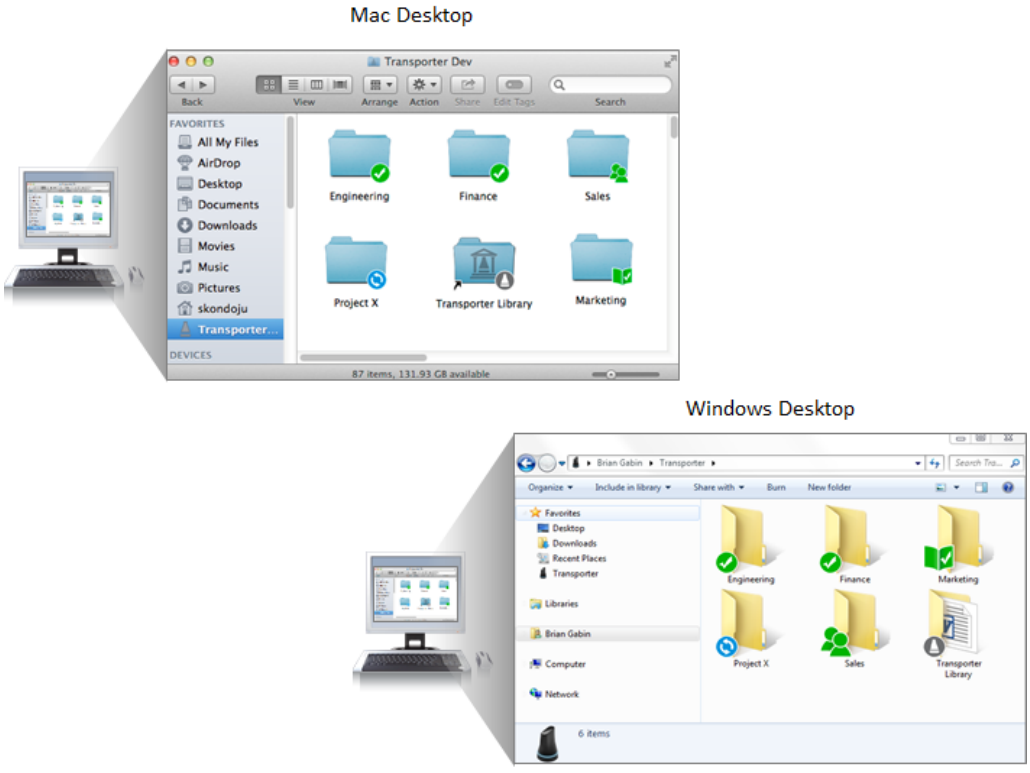
Transporter Folder

Transporter folders hold synced files for each user to access. Organization users can invite others to their shared folders. Items that are shared are indicated with a people icon; that icon turns blue to indicate that an item is syncing, and when the sync is complete the icon turns green. A book icon indicates that an item is read-only. When organization users select individuals with whom to share a file they can configure read-only or read-write privileges.

Transporter Library

The Transporter Library is where files are stored on Transporter appliances, and it is only available to organization users. When organization users access the Transporter Library folder, they are accessing the streaming version of the live file, not the locally cached version residing in the Transporter folder. The Transporter Library is synced between Transporters, but not to endpoint devices. Because the Transporter Library usually contains a larger, more complete set of corporate data, local access is essential.

Figure 1. Mac and Windows User Experience



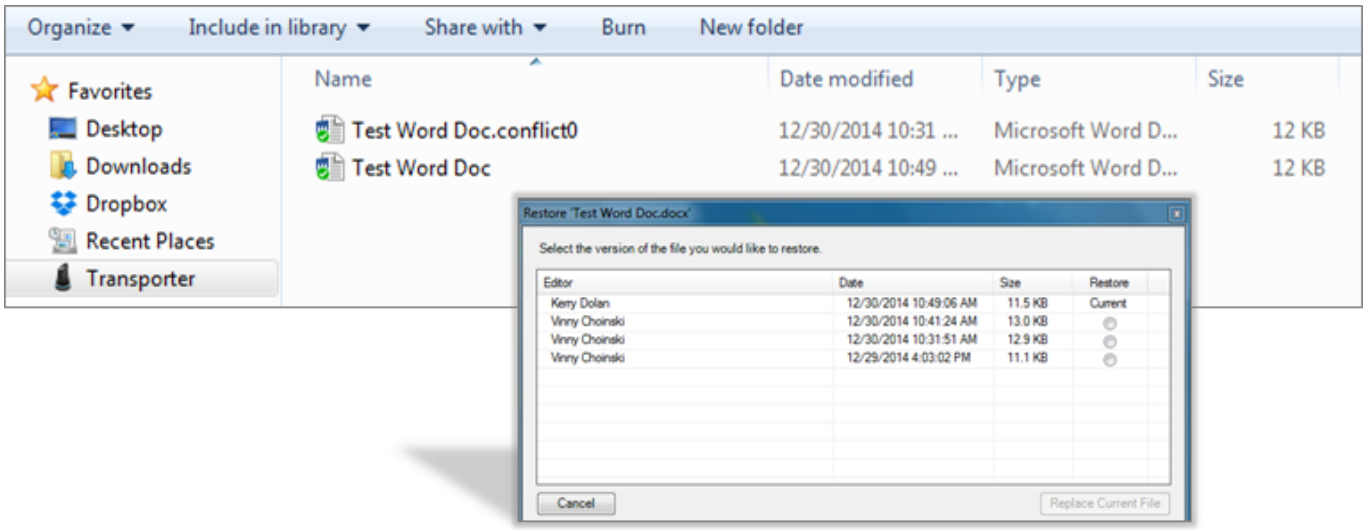
Modifying Documents

Documents that are in a shared folder can be modified (unless they are designated as read-only). When a user modifies a document, a notification appears on the desktops of users sharing that document. ESG Lab tested having two users (VC and KD) modify the same document (*Test Word Doc.docx*) at the same time. VC opened, edited, and saved the document before KD saved her edited version. As a result, two files were saved on desktops of both users: *Test Word Doc.docx* included VC's changes, and *Test Word Doc.conflict0.docx* included KD's edits. This method lets users know that a conflict exists so they can communicate to resolve it. The top screen in Figure 1 shows both documents on a Windows desktop.

Versioning and Restore

Users can easily view time-stamped versions of files that have been edited. ESG Lab tested this with the file *Test Word Doc.docx.* We right-clicked on the file name and were presented with the recent versions of the file, including one version listed as "current" and others that had been edited and saved (Figure 2). Simply by selecting a version we were able to restore it.

Figure 2. File Sharing and Collaboration Features

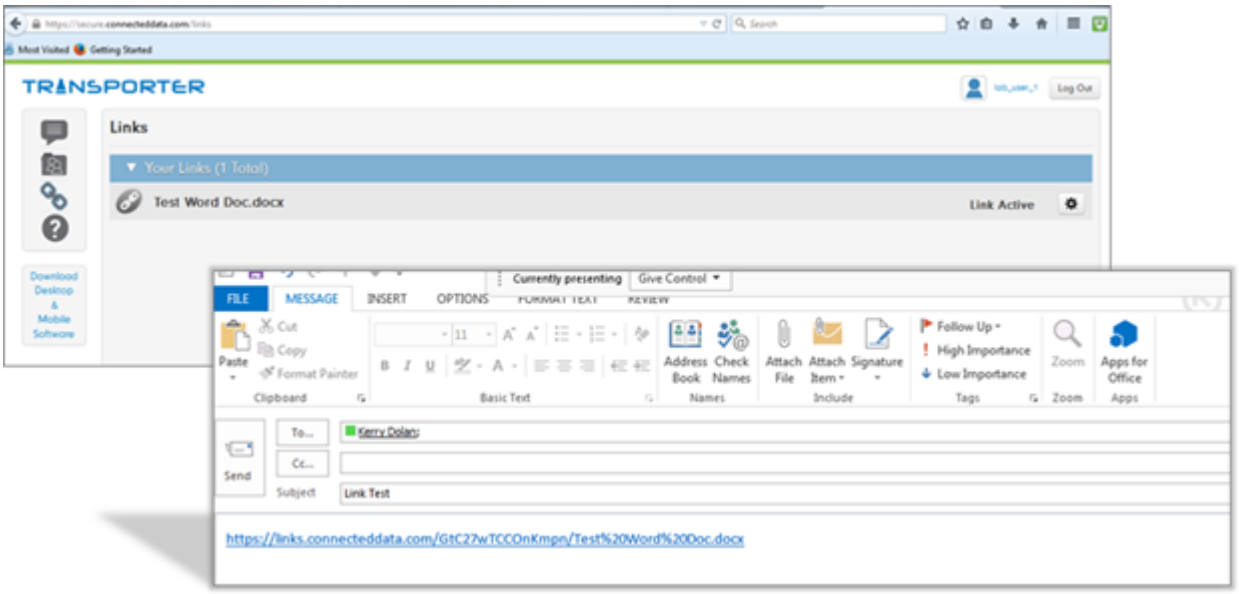


Links

Transporter offers two kinds of links to share files: direct and standard links. Direct links transfer files directly from a Transporter to the recipient, so that the files are never uploaded to Connected Data's servers. This type of link offers a higher degree of privacy, but also requires the recipient to install a small browser plug-in. Standard links upload files to Connected Data's servers and allow recipients to download them without a plug-in. While this type of link does not offer the same degree of privacy, it is easier to use. This can be especially useful for e-mailing links to clients who don't care to authorize or install anything.

As Figure 3 demonstrates, ESG Lab created a direct link from the VC account and emailed it to KD outside of our Transporter domain, thereby representing an external user. KD then clicked on the link, which took us to *links.connectedata.com*. There, a message indicated the document that was available, and that KD simply needed to download a plug-in to access it. The process was simple and fast.

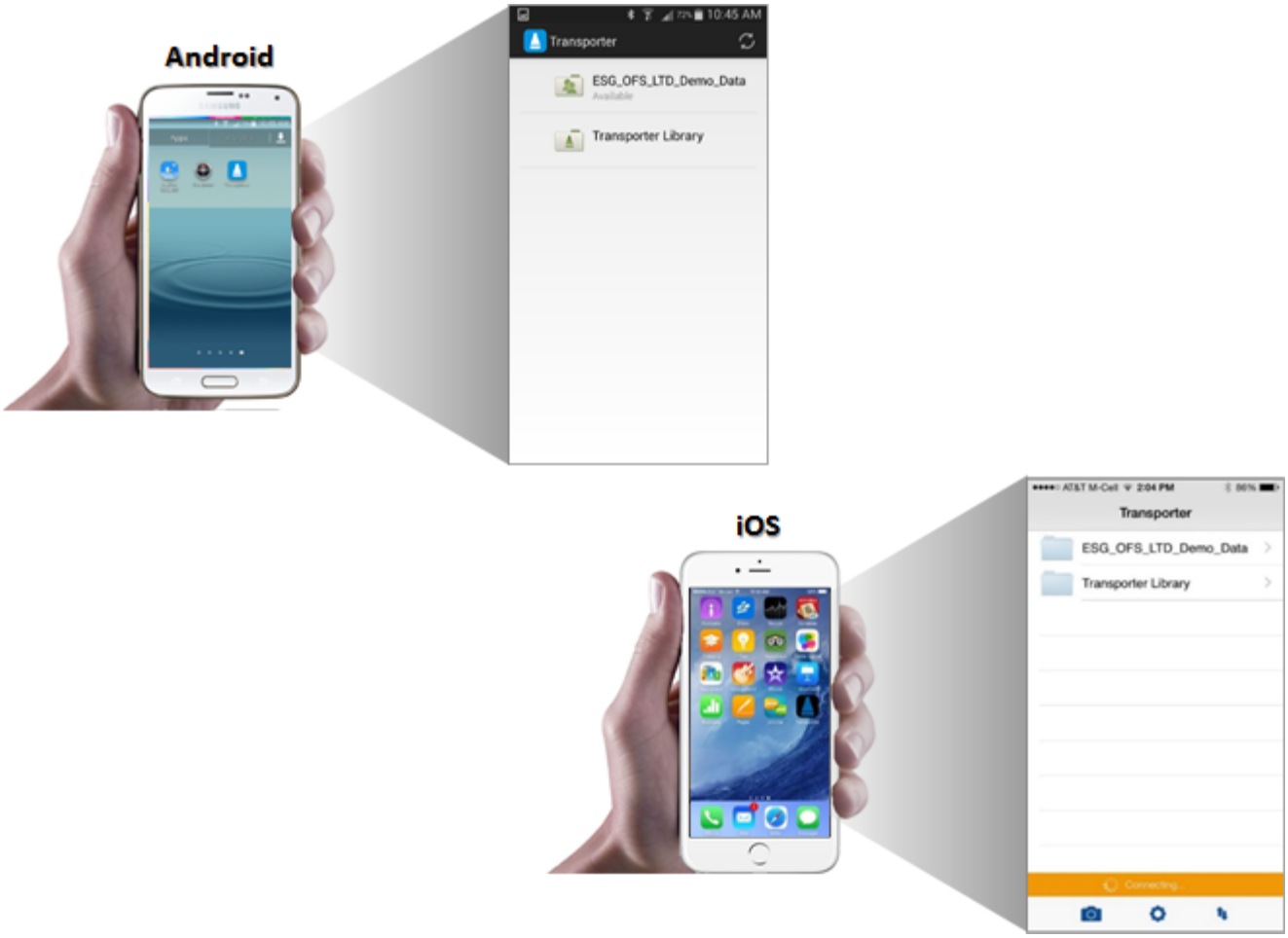
Figure 3. Link Management



The User's Perspective: Mobile Clients

Mobile devices including Apple iOS and Android are supported. Users simply download the Transporter application from the appropriate application stores and log in using their Transporter credentials. Once they are logged in, they can view their folders and files. On mobile devices, metadata and thumbnails are automatically synced, not full files. This keeps users from experiencing delays as they travel between networks with different capabilities, as well as unnecessarily consuming network bandwidth that they may be paying for. Users simply click on files to download and swipe from right to left to delete.

Figure 4. Mobile Users' Experience



The Administrator's Perspective

ESG Lab also tested the administrator functions. In a Transporter deployment, administrators set up the Transporters, claim and un-claim them, add, remove, manage organization users and groups, and manage access to files when users leave. Administrators can see all the Transporters that they have claimed, and can see and modify all organization and guest users. By drilling down on individual users, Transporter administrators can see all file links in play. These can be expired manually. (The ability to configure automatic file retention time is on the product roadmap.)

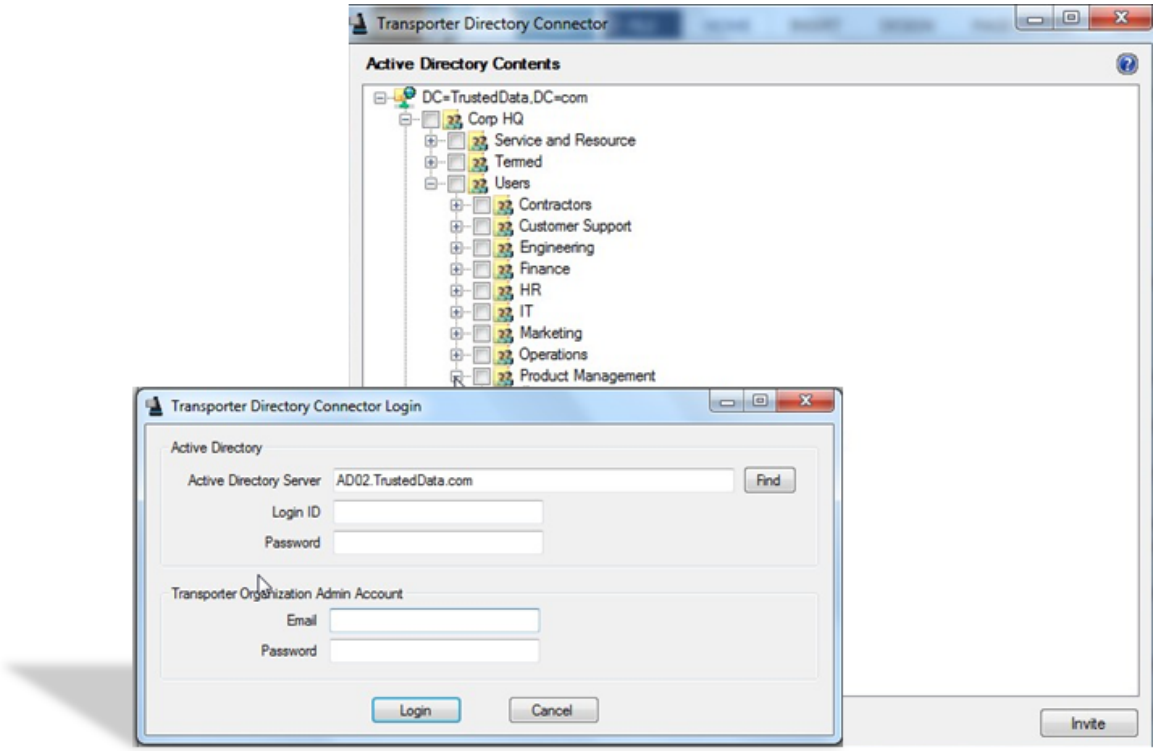
The administrator screen shows connected Transporters, plus details about storage capacity, IP addresses, network ports, versions, activation dates, disk usage, and folders. Creating new users is simple and fast. Administrators can use the Transporter Directory Connector to automatically create accounts using the Active Directory domain. Alternatively, administrators can manually invite users using e-mail addresses.

Administrators can view file links on each Transporter, including their active status, and with a drop down box, each link can be copied or deleted.

Active Directory Integration

Transporters can be integrated with Active Directory (AD), simplifying administration and enabling single sign-on for users. Administrators can connect to the AD server and invite users into Transporter from the AD controller; individuals or groups can be invited. Large groups can be easily tracked for invitation status. Figure 4 shows the Active Directory domain and Transporter Directory Connector Login that ESG Lab tested.

Figure 5. Active Directory Integration

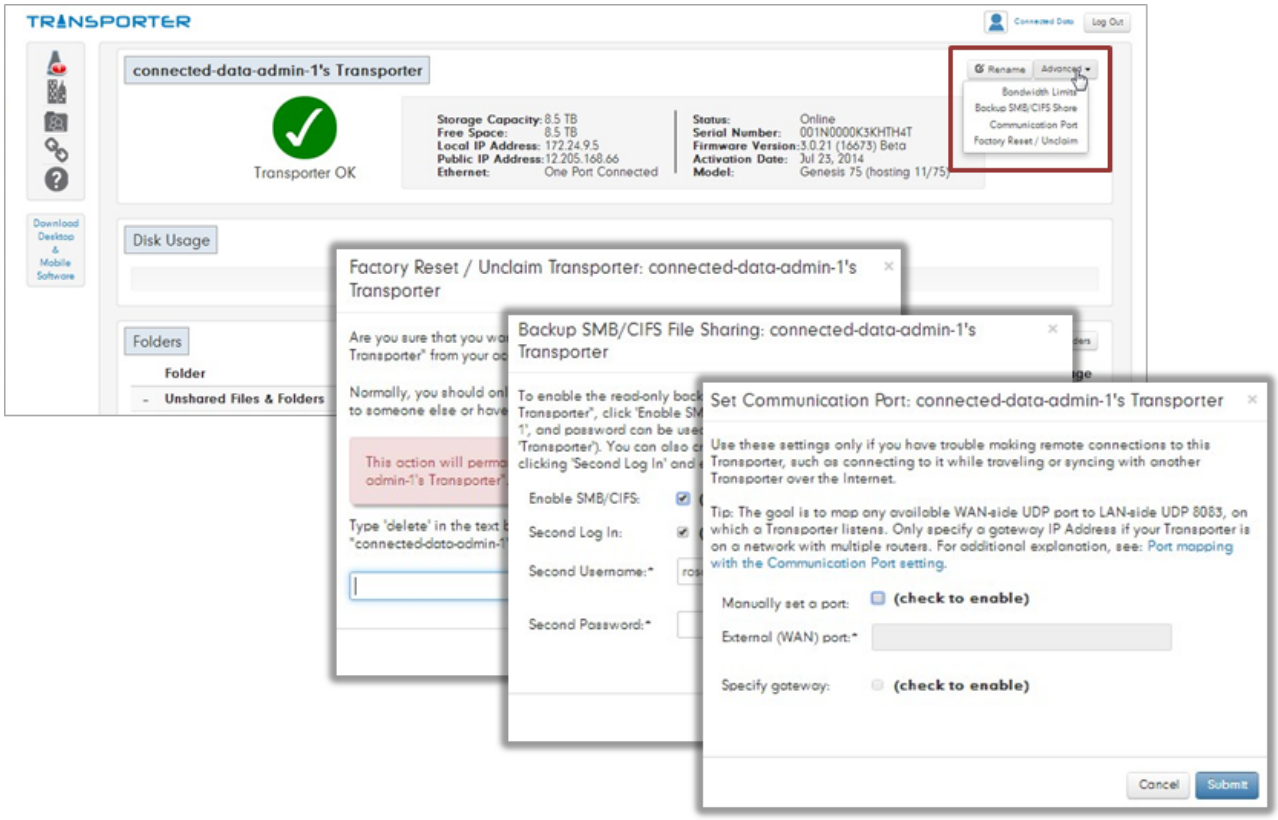


Advanced Features

The ***Advanced*** tab enables configuration of bandwidth, backup shares, and communication ports, as well as Factory Reset/Unclaim Transporter, which deletes all data stored on the Transporter. Administrators can drill down on specific groups, identify member access and status details, and identify which Transporters are connected to which users. Transporter does not require a fixed IP address or network port—it can use DHCP and ports based on availability. However, administrators can specify both IP addresses and network ports to ensure smooth network functionality.

Transporter appliances can be backed up using a password-protected, read-only CIFS share. Transporter will make automatic changes to the backup share, and then your backup application can back up that share along with the rest of your infrastructure. Replication occurs in real time; when you drag and drop a file onto a Transporter appliance, the global file system launches a replication process. Figure 5 shows the Administrator screen with the ***Advanced*** tab drop-down menu highlighted in red, along with the Factory Reset, Backup, and Set Communication Port dialog boxes.

Figure 6. Advanced Administration Features



Why This Matters

Simple, easy-to-manage file sharing for collaboration and improved productivity has become an expected part of the user experience in today's corporate environments. However, organizations struggle to control unintended access to sensitive corporate data while maintaining expected performance characteristics. In fact, when asked about factors driving interest in the ability to retain file data on-premises, more than half of both current public cloud model OFS users and potential hybrid or on-premises model OFS adopters indicated they wanted flexibility and control over where data is stored.[2]

The ESG Lab Test Drive validated the ability of Transporter to deliver the easy file sync and share features that users are demanding, but in a private cloud environment with full IT control and data protection. ESG Lab validated typical syncing and share functionality along with simultaneous user editing, creation of links for sharing with external users, and mobile device access. The Lab also validated administrative features, including the ability to integrate with Active Directory for access control, set up CIFS backups, configure ports, and execute a Factory Reset to remotely wipe a Transporter. These features demonstrate the business-class focus of Transporter, for both users and administrators.

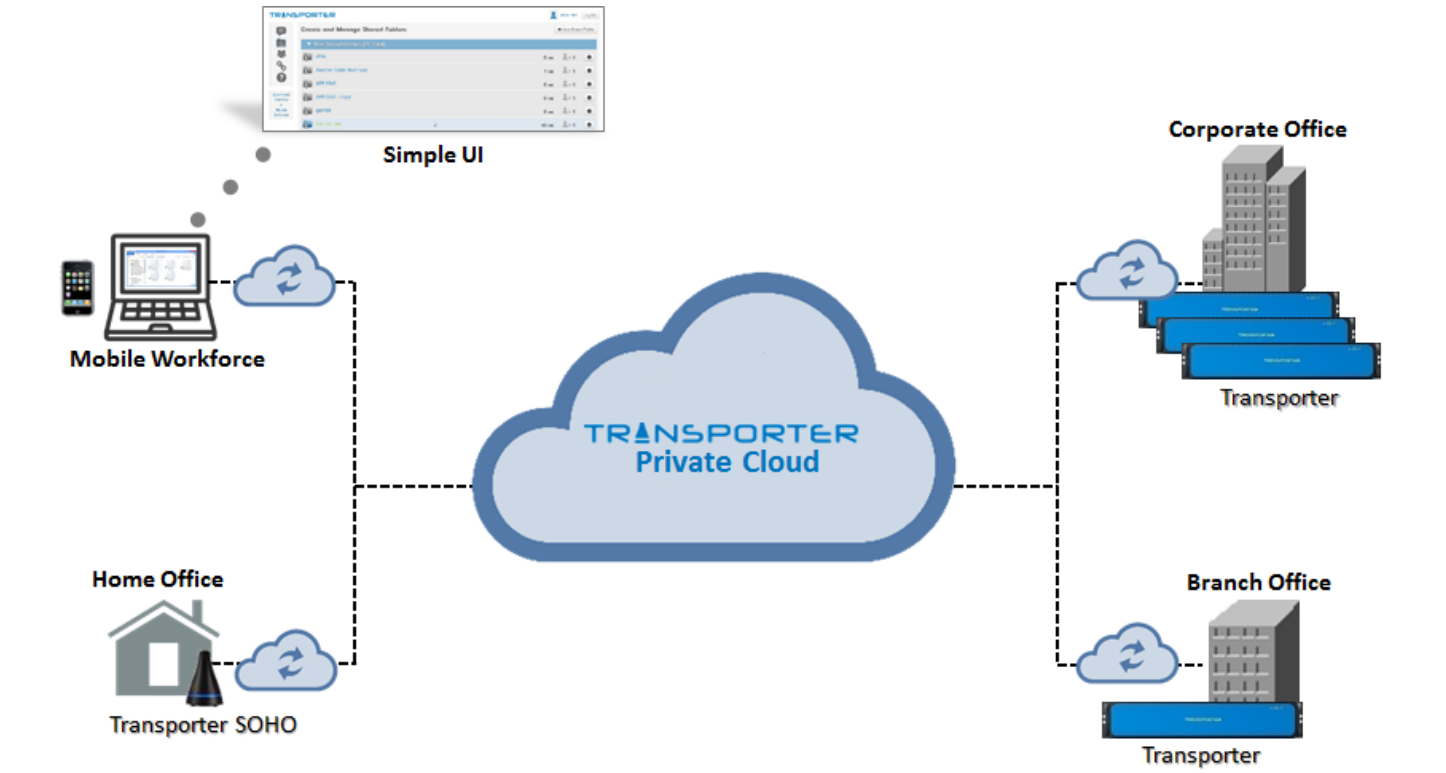
[2] Source: ESG Research Report, *Online File Sharing and Collaboration: Deployment Model Trends*, February 2014.

Cost-efficient, Distributed, Private-cloud Transporter Deployments

A key benefit of Transporter deployments is that organizations can create private clouds without excessive cost, leveraging the distributed nature of Transporter appliances designed for mid-range enterprise, SMB, and SOHO environments. Connected Data's first Transporter was designed for SOHO environments, to enable LAN-speed access to documents without having to go through the pain of a VPN. The addition of the rack-mount Transporters for mid-range enterprises and the desktop Transporter 15 and 30 for SMBs and remote offices makes Transporter a multi-level file sync and share solution that is affordable for any organization, and offers an upgrade path for additional features, performance, and capacity. Transporters are easy to scale, and organizations that started with a SOHO or SMB device can grow into the rack-mount product, and add units as needed to scale and protect data.

Here is an example of how Transporter's distributed deployments can benefit customers. An organization may have a Transporter rack-mount deployment at corporate headquarters for all corporate files. This enables LAN-speed access to any content, plus all the sync and share features. In addition, a branch office may have another Transporter with data replicated between the headquarters and branch office; this enables branch-office access to all corporate data at LAN-speeds instead of WAN speeds. Users have their own syncing folders on their desktops for local speed for those files that they are actually using. A home office user can have a SOHO version of the Transporter, with the same replication from HQ as the branch office, plus the local access on their device. And finally, users can travel with their mobile devices with file syncing and sharing capabilities. Figure 5 demonstrates how the same private cloud enables all of these deployments, delivering the features that end-users demand while ensuring the protection, security, and control of corporate IT.

Figure 7. Distributed Architecture



Why This Matters

While most organizations want to fully control their data, many small enterprises believe that a private cloud is beyond their reach from both financial and operational perspectives. Small organizations may have little or no IT staff, making a private cloud seem impossible to operate. In addition, small organizations and branch offices often believe that hardware and software are simply too expensive.

Connected Data's Transporter line starts small, with the SOHO appliance for individuals, redundant desktop models for groups and small businesses with up to 30 users, and the rack-mount Transporter models that currently support up to 150 organization users per appliance. Connected Data enables organizations to start small and grow with a private cloud that enables syncing and sharing of all file data among all your devices, data protection, full IT control, and no monthly fees. Connected Data makes distributed private clouds affordable for any organization, delivering the enterprise-class features they need.

The Bigger Truth

Today's IT end-users have begun to feel somewhat entitled. They are accustomed to fast networks, virtual machines that can be spun up in minutes, smartphones and tablets, and generally having access to whatever they want, whenever they want it. And why shouldn't they be? Organizations are constantly pushing employees to be more productive, and technological advancements can make that happen.

They have also become accustomed to accessing data with consumer-focused public-cloud sync and share solutions. These accounts are easy to get—free for sharing and syncing data with a small amount of storage, easy to upgrade with just a credit card, and easy to use. As a result, many end-users are turning to these solutions when they become impatient with technologies that slow them down or make things complicated. They don't want to wait for IT to increase their storage capacity, and they don't want to wade through complex security procedures for VPN access that often comes with restrictions. So what do they do? They put their data in a public cloud without IT's knowledge.

And that's where the problems begin. These solutions are outside of the IT domain and its control, security, and protection. IT has no idea what corporate data is stored outside their domain, who users are sharing with, whether backups are up to date and secure, and what data is vulnerable once users leave. It's like the Wild West out there, and IT organizations have little recourse.

At this point, there is no putting the genie back in the bottle. But what organizations *can* do is provide the same usability and access benefits in a private-cloud solution that is managed by IT. Connected Data Transporter offers these features in a solution designed for departmental and small enterprises. Transporter stores corporate data on private hardware that IT configures and operates, with enterprise features but at an affordable price point. These appliances are easy to acquire, install, and operate, and offer business-focused architectural advantages such as redundant hardware, SSD metadata acceleration, single instancing per device, AES 256 encryption for data in flight, and automated, real-time syncing between authorized devices. Organizations can put Transporters at multiple locations and can integrate them with corporate access management frameworks such as Active Directory. IT can configure networks and bandwidth, back them up, and remotely wipe them for complete protection.

Connected Data began in the SOHO market with their smaller Transporter desktop devices, giving them a good handle on understanding individual user needs. These individual Transporters and the desktop SMB Transporters can be integrated with the rack-mount Transporter models, giving users easy access to synced files at headquarters locations, branch offices, and home offices. With Transporter, Connected Data has done a good job of including key features that address *business* needs as an entry into the larger business market. There are solutions from other vendors that offer larger feature sets and have deeper integration with enterprise applications and infrastructures, but these are focused on the large enterprise market that is not Connected Data's target.

ESG Lab's Test Drive validated the desktop and mobile client features for end-users as well as the architecture, security, and control features for IT administrators. We can validate that this is a true business solution that solves the challenges of security and control while providing fast sync and share access to file data in a distributed environment. Transporter is an affordable, private-cloud solution that delivers on key business requirements.