Enterprise Strategy Group | Getting to the bigger truth.™

ESG Lab Review

Extenua Cloud2Drive: Secure Access—Simplified

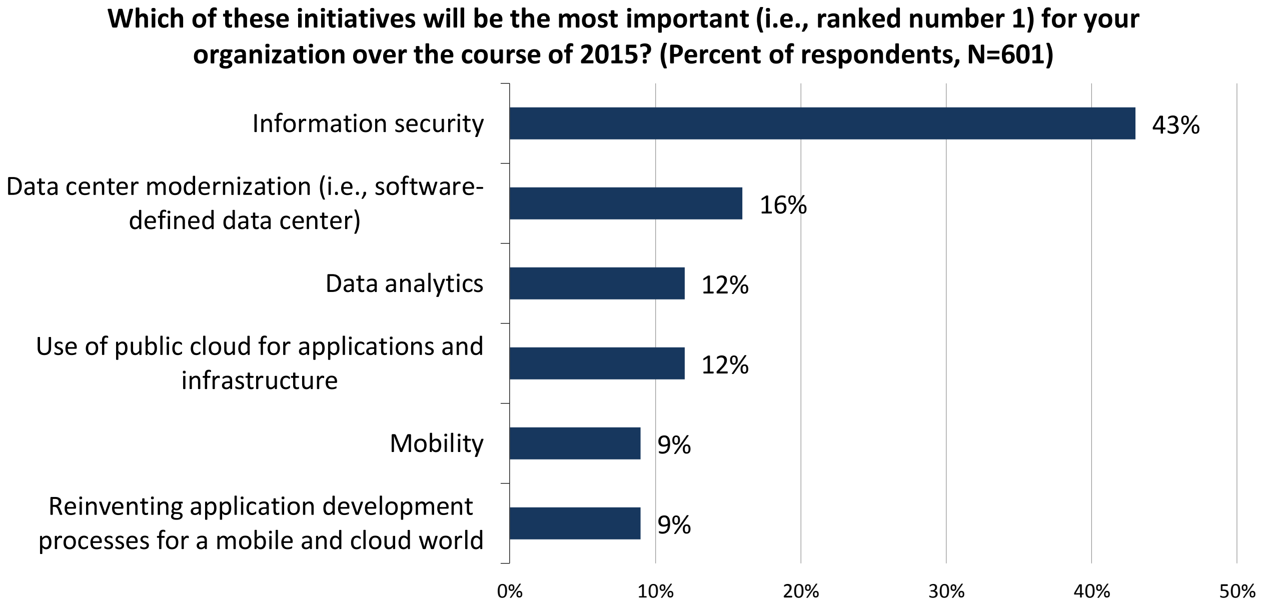
Date: July 2015   **Author:** Jack Poller, Lab Analyst

Abstract: *This ESG Lab Review documents hands-on testing of Extenua Cloud2Drive, an enterprise file sync and share (EFSS) solution providing security, simplicity, and aggregation of cloud storage providers. Extenua designed Cloud2Drive to provide levels of security exceeding current federal requirements. By virtualizing cloud storage across multiple providers, Cloud2Drive enables organizations to simplify cloud storage, eliminate single points of failure, and ensure universal access to corporate data.*

The Challenges

IT has long understood the data security threats to their organizations such as unauthorized access, viruses, malware, data collection, and exfiltration. Cyber-criminals are adept at creating new and insidious methods of infiltrating data infrastructures. Advanced malware attacks wreak havoc in many ways, from stealing data to shutting down operations, and today's attacks are far more sophisticated and difficult to prevent than ever before. ESG research revealed that cybersecurity is such an important issue that information security far outweighs all other concerns at the top of the "CIO whiteboard" of initiatives and technology meta-trends (see Figure 1).[1]

Figure 1. "CIO Whiteboard" Initiatives



Source: Enterprise Strategy Group, 2015.

As a first line of defense, network architects employ encryption to protect and secure data that must travel over insecure links, using industry-standard protocols such as IPsec to protect site-to-site communications. However, no system can be 100% successful in eliminating vulnerabilities. This is especially true in the modern data center, where

[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.

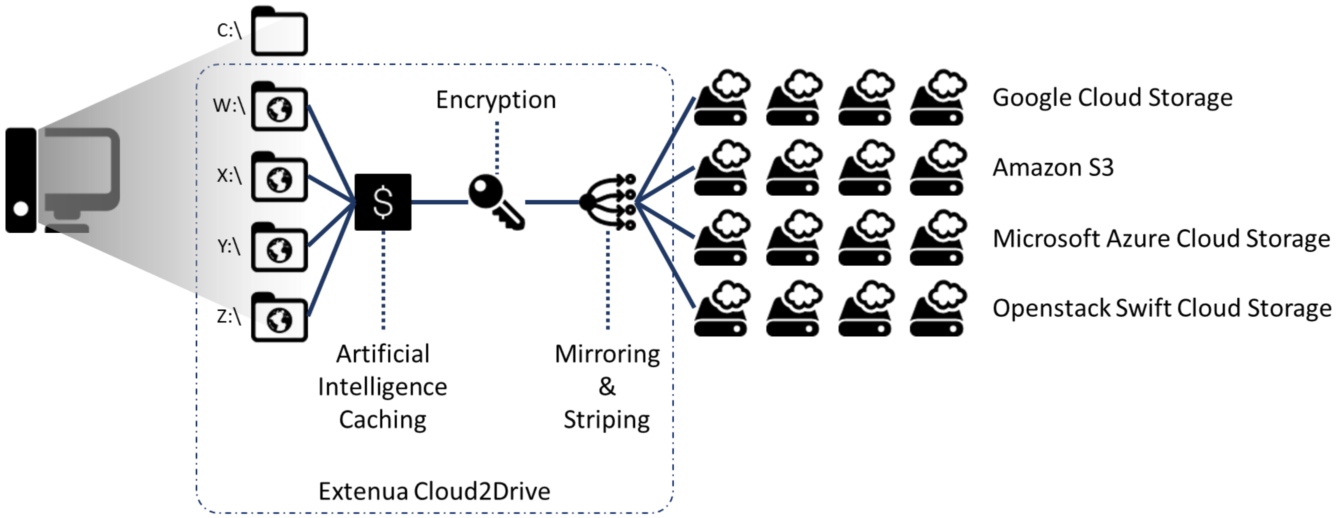
The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments. This ESG Lab report was sponsored by Extenua.

enterprises are leveraging the power of infrastructure-as-a-service (IaaS), shifting from local storage to cloud storage to reap the benefits of universal data availability through enterprise file sync and share applications. Malicious actors can use phishing attacks, compromised devices, and other exploits to gain access to an organization's data and intellectual property through cloud storage administrator accounts.

The Solution: Extenua Cloud2Drive

Extenua Cloud2Drive is an enterprise file sync and share solution designed to provide extremely strong security, storage provider aggregation, flexibility, scalability, and file integrity. The Cloud2Drive application runs on both Windows workstations and servers, and Android- and iOS-based mobile devices, while the Manager application runs on Windows. When installed, Cloud2Drive presents cloud storage to the user using the native storage interface, e.g., as a network drive for Windows systems.

Figure 2. Extenua Cloud2Drive Architecture Overview



Extenua designed Cloud2Drive with enterprise-class features, including:

- **Security**—Cloud2Drive encrypts data in real time, on the fly during transmission to the cloud storage provider, and at rest, both at the provider and locally, ensuring that third parties cannot make sense of data. Using a patent-pending algorithm that harnesses content slicing and obfuscation, organizations deploying Cloud2Drive are compliant with all security mandates in PCI DSS, HIPAA, CASB1386, GLBA, DoD 5015.2, and other regulations. According to Extenua, using all available computing power, it would take 25 eons to break Cloud2Drive's data encryption.
- **Aggregation & Migration**—Cloud2Drive enables administrators to aggregate unlimited cloud storage from multiple providers to create virtual drives that scale to fit the needs of any organization. Administrators can build a storage pool by spanning data across multiple storage containers for performance and bandwidth aggregation, similar to traditional RAID 0. Alternatively, administrators can build a storage pool by replicating data to multiple storage containers for high availability and fault tolerance, similar to traditional RAID 1.
- **Flexibility**—Cloud2Drive is cloud-provider-agnostic, enabling a single virtual drive to use storage from different clouds. Access is unrestricted from any location, eliminating the need for additional hardware VPNs or tokens.
- **Ease of Use**—Utilizing the native OS file structure, Cloud2Drive requires no change in user behavior. Cloud2Drive appears to the user just like a standard network drive. Administrators can script the automatic deployment of Cloud2Drive across the organization, and can import user profiles from Active Directory.
- **Availability**—Cloud2Drive incorporates an artificial intelligence engine to optimize local caching of data from virtual drives. The AI engine learns how each user works with files, profiling each user's individual activity. Then

Cloud2Drive can predict which files each user will need, and cache those files on local storage. According to Extenua, the AI engine is 99% accurate in determining which files to cache, enabling workers to embrace the work anywhere, anytime, from any device mentality with confidence that they will have access to all their critical files.

- **Integrity**—Cloud2Drive's patent pending data corruption prevention algorithm prevents accidental data overwrite and incidental data loss using distributed file locks to actively and effectively ensure data integrity at all times.

ESG Lab Tested

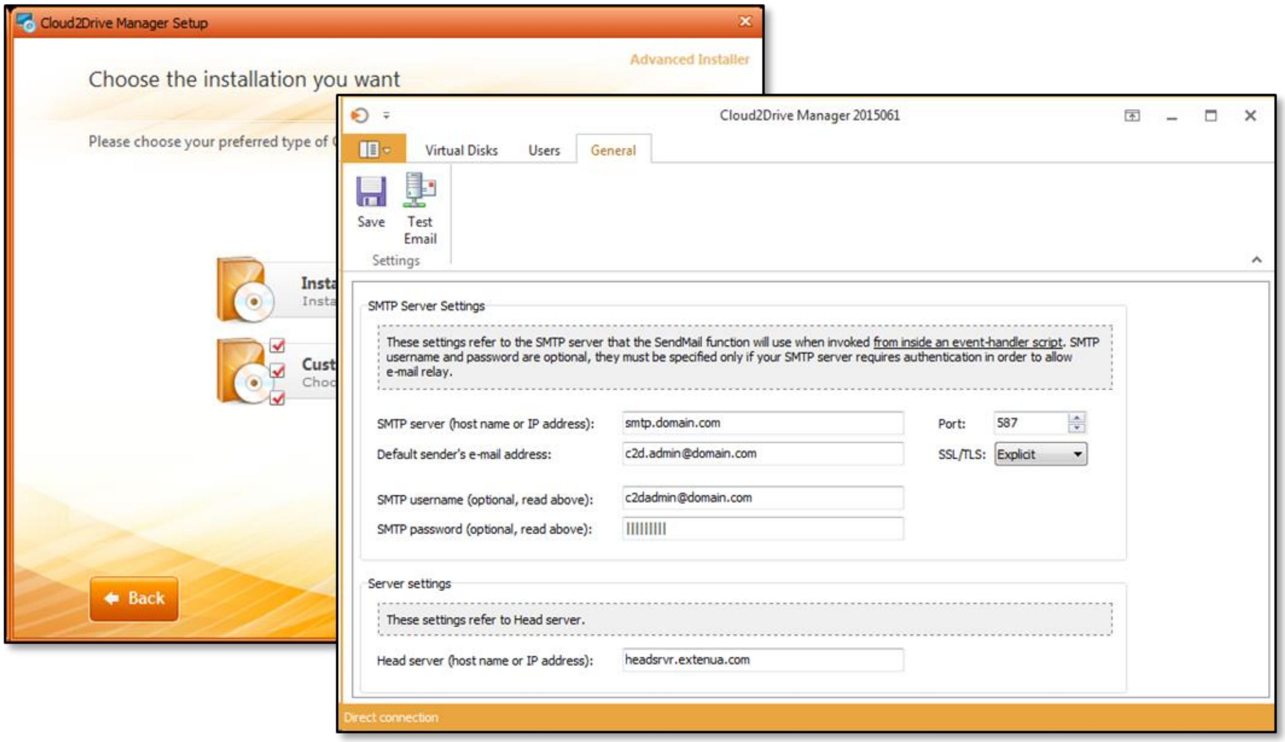
ESG Lab performed hands-on testing of Extenua Cloud2Drive with a goal of validating the features that make it a secure, easy to use, and flexible EFSS solution for scalable data security and privacy in today's multisite environments.

Cloud2Drive Installation and Configuration

The Cloud2Drive solution includes client software for Windows, Android, and iOS, and a separate Cloud2Drive Manager administrator package for Windows. First, ESG Lab downloaded and installed Cloud2Drive Manager on a Windows 7 workstation. Installation required agreeing to the software license and optionally specifying the installation location, and completed in less than a minute.

The first step of configuration consisted of providing e-mail server and login information, enabling the manager console to send mail to users on behalf of the Cloud2Drive instance, as shown in Figure 3.

Figure 3. Cloud2Drive Manager Installation and Configuration



Choose the installation you want

Please choose your preferred type of

SMTP Server Settings

These settings refer to the SMTP server that the SendMail function will use when invoked from inside an event-handler script. SMTP username and password are optional, they must be specified only if your SMTP server requires authentication in order to allow e-mail relay.

SMTP server (host name or IP address): smtp.domain.com
Port: 587
Default sender's e-mail address: c2d.admin@domain.com
SSL/TLS: Explicit
SMTP username (optional, read above): c2dadmin@domain.com
SMTP password (optional, read above): |||||||||

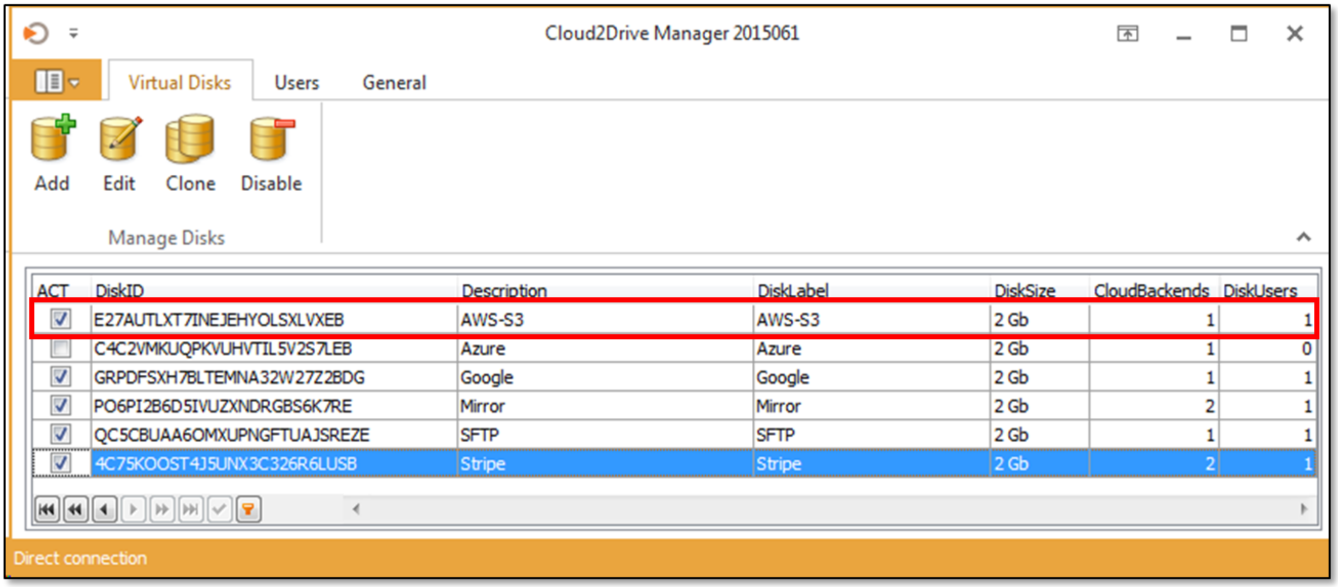
Server settings

These settings refer to Head server.

Head server (host name or IP address): headsrvr.extenua.com

The next step was to create virtual disks. Selecting the ***Virtual Disks*** tab displayed the list of existing virtual disks (Figure 4). The ***Virtual Disks*** tab displayed a table of all configured virtual disks, including the universally unique identifier (UUID), the description and disk label, the disk size, number of cloud backends and users, and whether or not the virtual disk is active.

Figure 4. Configure Virtual Disks



ACT	DiskID	Description	DiskLabel	DiskSize	CloudBackends	DiskUsers
☑	E27AUTLXT7INEJEHYOLSXLVXEB	AWS-S3	AWS-S3	2 Gb	1	1
□	C4C2VMKUQPKVUHVTIL5V2S7LEB	Azure	Azure	2 Gb	1	0
☑	GRPDFSXH7BLTEMNA32W27Z2BDG	Google	Google	2 Gb	1	1
☑	PO6PI2B6D5IVUZXNDRGBS6K7RE	Mirror	Mirror	2 Gb	2	1
☑	QC5CBUAA6OMXUPNGFTUAJSREZE	SFTP	SFTP	2 Gb	1	1
☑	4C75KOOST4J5UNX3C326R6LUSB	Stripe	Stripe	2 Gb	2	1

ESG Lab selected ***Add*** to add a new virtual disk. The first step included specifying the disk label, which is visible in the Windows file explorer and helps to identify the various Cloud2Drive virtual disks to the user. In this case, we named the virtual disk "AWS-S3" to indicate a virtual disk using Amazon S3 cloud storage as the backend. ESG Lab also provided a description of the disk, the disk size, and the mount letter.

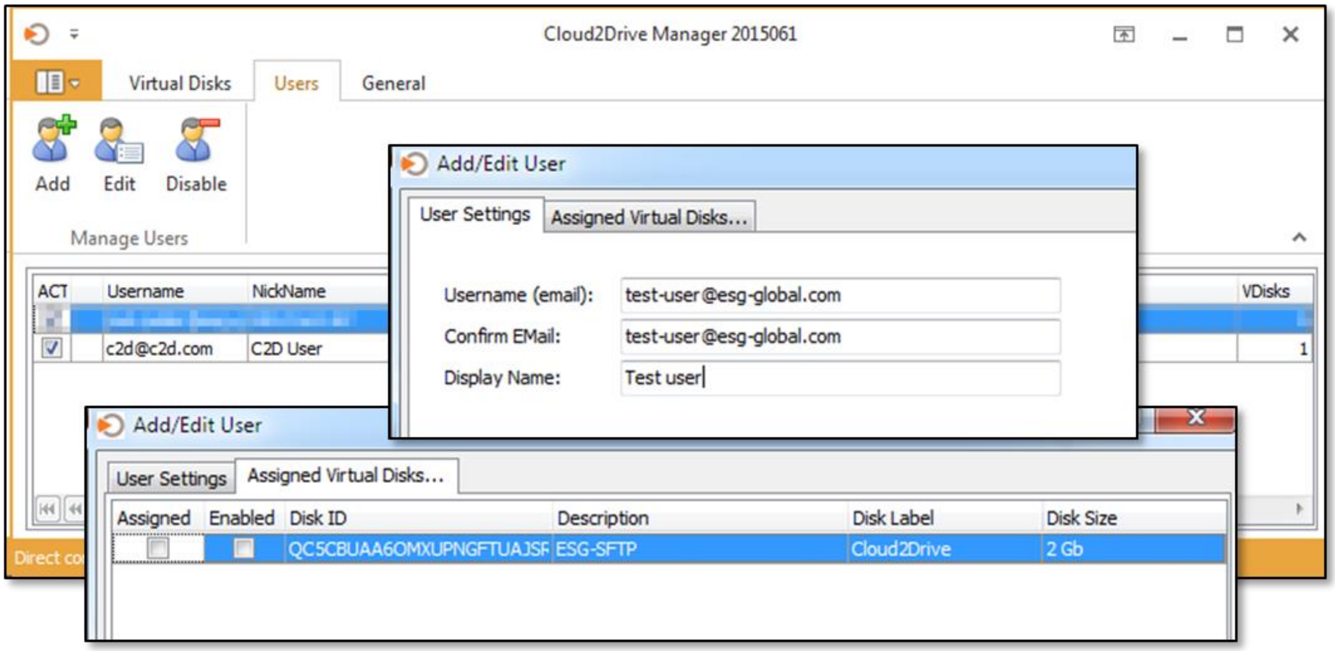
Since Cloud2Drive is a storage virtualization engine, administrators can alter the virtual disk size at any time. For example, an administrator can scale a virtual disk from 1TB to 1PB simply by editing the virtual disk, and changing the size parameter from 1000GB to 1000000GB.

ESG Lab clicked ***Save*** to save the basic configuration information for the virtual disk. Next, ESG Lab selected the ***Backend Cloud Storage*** tab to add cloud storage backends to the virtual disk. This brought up the list of already configured backend storage providers. Next, we clicked on the ***+*** symbol at the bottom to add a row to the storage provider table, and then selected S3 as the storage provider type and entered the Amazon S3 keys for our storage container. Extenua provides documentation on the mapping of keys for containers from each storage provider to their respective Cloud2Drive parameters. We then saved the storage configuration.

The administrator can decide to pool multiple cloud storage containers using striping (similar to RAID 0), or mirroring (similar to RAID 1), simply by selecting either option using a radio button. When configuring the storage pool for striping, the administrator can assign a percentage of data to reside on each container.

The final step in configuring a virtual disk was assigning users to the disk. This can be accomplished from both the ***Assigned to Users*** tab of the virtual disk add/edit pane, or from the Users pane. ESG Lab saved the virtual disk configuration information, and then selected the ***Users*** tab to add a new user, as shown in Figure 5.

Figure 5. Add/Edit User



ACT	Username	NickName	VDisks
[redacted]			
☑	c2d@c2d.com	C2D User	1

Username (email): test-user@esg-global.com
Confirm EMail: test-user@esg-global.com
Display Name: Test user

Assigned	Enabled	Disk ID	Description	Disk Label	Disk Size
☐	☐	QC5CBUAA6OMXUPNGFTUAJSF	ESG-SFTP	Cloud2Drive	2 Gb

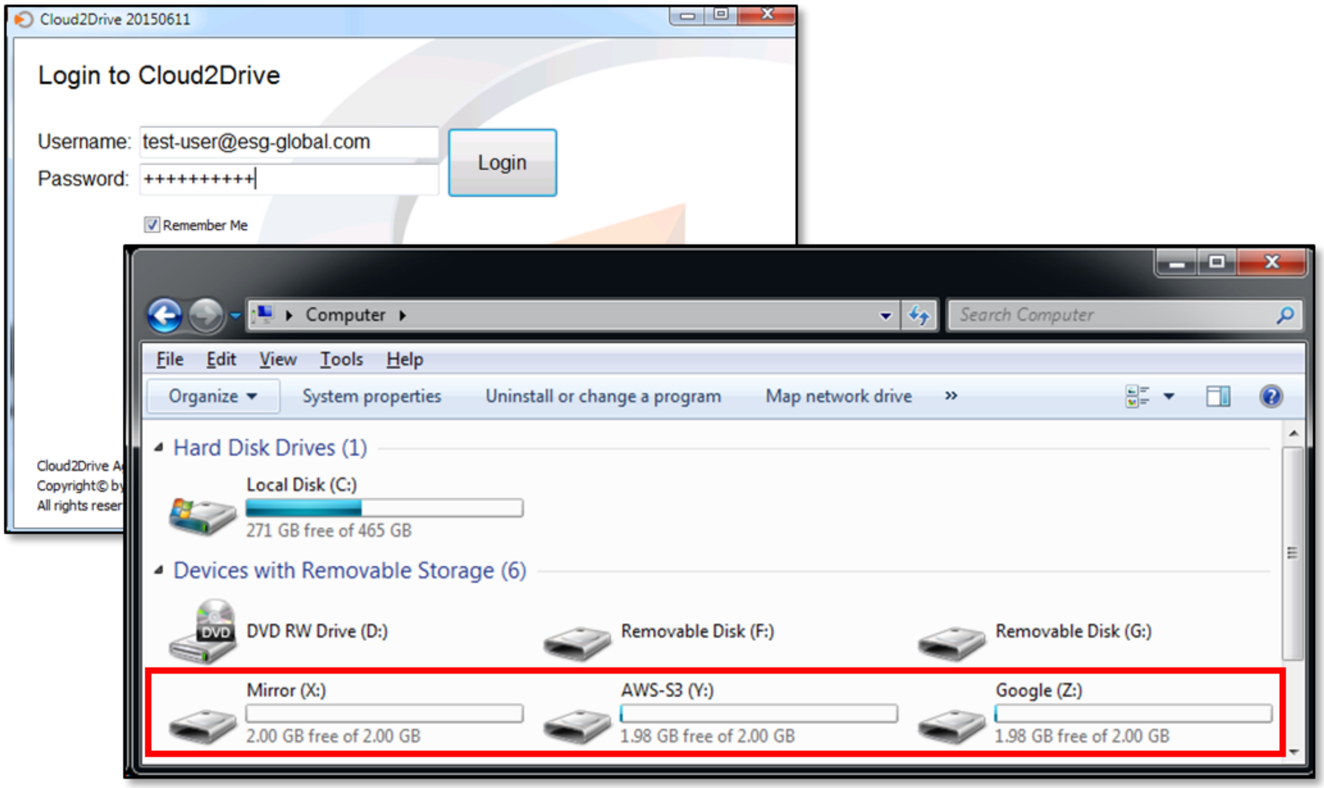
Similar to the ***Virtual Disk*** tab, the ***Users*** tab provides a table listing all users, as well as buttons to add, edit, and enable/disable users. ESG Lab selected ***Add*** to add a new user. The ***Add/Edit User*** window had tabs for ***User Settings*** and ***Assigned Virtual Disks***. On the ***User Settings*** tab, ESG Lab entered "Test user" and "test-user@esg-global.com" for the user's name and e-mail address. When we saved the user information, Cloud2Drive assigned a default password and sent a welcome e-mail to the test user. The test user was required to change the password on first login. Next, ESG Lab selected the ***Assigned Virtual Disks*** tab and assigned the ESG-SFTP virtual disk to the test user.

Cloud2Drive stores the configuration of all virtual disks and all users in the Extenua cloud, ensuring that configuration information is always available to any Cloud2Drive Manager or client.

Once ESG Lab configured the virtual disks and users, we downloaded the Cloud2Drive client software from the Extenua website. Installation on the same Windows 7 workstation was easy, with the location of the software as the only available option, and completed in less than a minute.

Next, using the welcome e-mail with the temporary password sent by the Cloud2Drive manager, ESG Lab logged into Cloud2Drive as a user. As required, we changed the password, logged out, and logged in again (Figure 6). Once we logged in, the Cloud2Drive icon was visible in the Windows taskbar or system tray. This icon is used to issue notifications to the user, and to exit Cloud2Drive.

Figure 6. Cloud2Drive User View



Login to Cloud2Drive

Username: test-user@esg-global.com

Password: ++++++++++

☑ Remember Me

After logging in, Cloud2Drive mounted the virtual disks as network shares as specified by the user and virtual disk configuration of the Cloud2Drive Manager. We assigned drive letter X to a virtual disk using mirrored storage from Microsoft Azure and Google Cloud Storage. Drive letter Y was assigned to the virtual disk using Amazon S3, and drive letter Z was assigned to a virtual disk using Google Cloud Storage.

Why This Matters

According to ESG research, training administrators and users on new tools and processes was the second most-cited challenge (after security) reported by organizations who have deployed an enterprise file sync and share system.[2] Ease of use is especially important for a corporate on-premise file sharing solution intended to replace the free online file sharing (OFS) solutions that employees use without the knowledge of IT. Unless that new solution is easy to use and provides the features that users require, employees may continue to use insecure public OFS applications, risking data leaks and account compromises, potentially exposing all corporate data.

ESG Lab validated that Extenua Cloud2Drive was easy to use and deploy with a clean, uncluttered GUI. For administrators, creating virtual drives with any combination of cloud storage containers from Microsoft, Google, Amazon, and Openstack was quick and easy. Creating and maintaining user accounts was equally simple and fast.

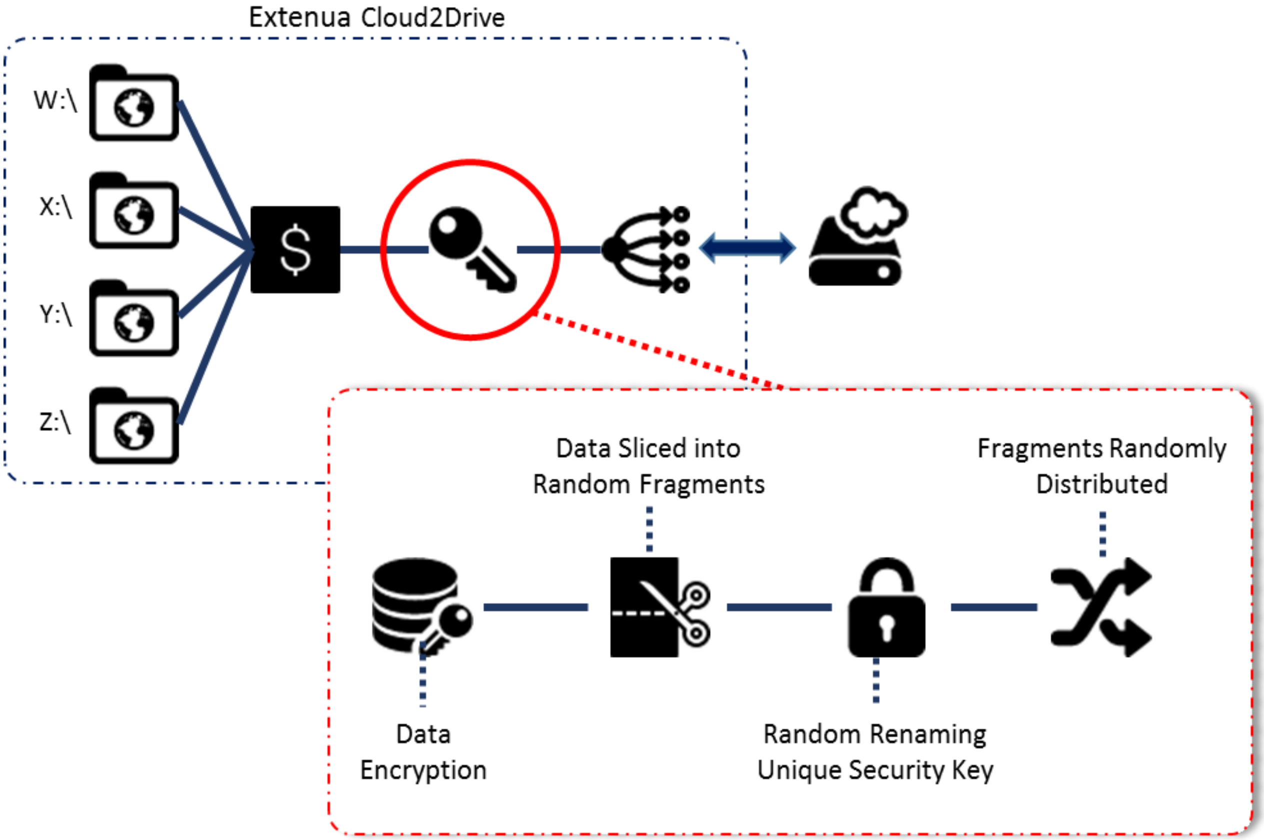
Because Cloud2Drive presents cloud storage as a local drive, users don't have to change their behavior. This helps to encourage users to forego insecure public OFS solutions in favor of the secure Cloud2Drive EFSS solution. The ease of deploying, configuring, and maintaining the Cloud2Drive EFSS solution, combined with extensive security enables administrators to spend less time managing the EFSS environment, freeing critical resources to focus on managing and securing other critical parts of the IT infrastructure.

Built-in Data Protection and Security

Extenua Cloud2Drive provides extensive security and built-in data protection, ensuring that corporate data is not exposed to malicious actors or the public, even when using multiple public-cloud storage providers. As shown in Figure 7, Cloud2Drive implements a multi-phase encryption and obfuscation algorithm to prevent unauthorized users from assembling and decrypting the data.

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

Figure 7. Cloud2Drive Encryption and Obfuscation


Extenua Cloud2Drive
W:\
X:\
Y:\
Z:\
Data Sliced into Random Fragments
Fragments Randomly Distributed
Data Encryption
Random Renaming Unique Security Key

Here are the steps taken to secure data written to the cloud:

1. Data is encrypted locally and stripped of its digital identity.
2. Using a patent-pending algorithm, data is then sliced into randomized fragments.
3. Each fragment is randomly named and then issued a unique security key.
4. Fragments are scattered across randomly generated directories.
5. Data transmitted to cloud storage is once more encrypted over the wire, using secure Internet data transmission protocols.
6. Data is encrypted at rest in the cloud using the cloud storage providers' native encryption schemes.

In addition to being extremely hard to crack (Extenua calculated that it would take 25 billion years using all known computing power), Cloud2Drive's strong encryption and obfuscation scheme is compliant with all current security mandates for PCI DSS, HIPAA, CASB1386, GLBA, DoD 5015.2, and other data protection regulations. If a cloud storage administrator account is compromised, malicious actors almost assuredly cannot re-assemble and decrypt the data.

Security is further enhanced using Extenua's best practices, including striping data across multiple cloud storage providers, and partitioning corporate data across multiple virtual drives, enabling administrators to grant access for critical data to only the small group of users who need it.

Why This Matters

With recent high-profile malware attacks resulting in significant data loss and interruptions of operations, many organizations are realizing that they are vulnerable to malware and advanced threats. As organizations become more dependent on cloud infrastructures and enterprise file sync and share solutions, they are increasingly susceptible to attacks, especially those targeting the extraction of corporate data and intellectual property.

ESG Lab confirmed that Extenua Cloud2Drive's heavyweight encryption scheme encrypts and obfuscates data on the fly, at rest on the local hard drive, and when stored in cloud storage. According to Extenua, it would take 25 eons to brute-force crack the encryption, and, combined with the obfuscation scheme, it is nearly impossible to correlate data in the cloud with the original data. This ensures that, if the administrator privileges to cloud storage accounts are compromised, data security is still maintained, providing peace of mind to administrators and managers.

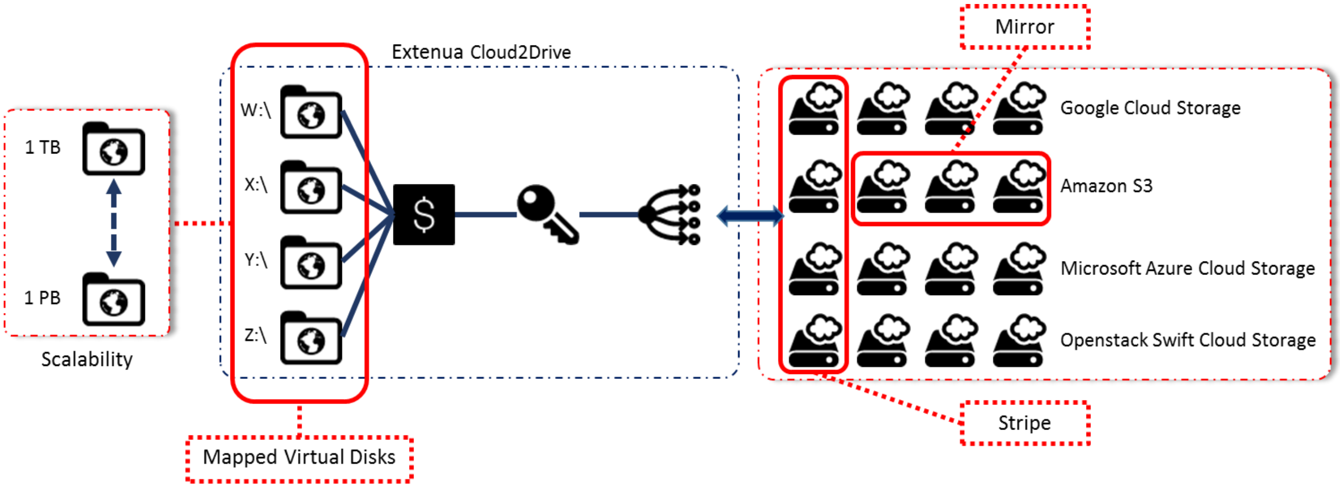
Virtually Unlimited Scalability

Extenua Cloud2Drive aggregates an unlimited number of cloud storage containers to create a storage pool that scales to fit the needs of even the largest enterprises. Storage pools can be aggregated in single or multiple virtual drives, which are used natively on client platforms. As shown in Figure 8, a virtual disk can be scaled in size, and can be backed by mirrored or striped cloud storage containers, providing high availability, redundancy scalability, and migration between cloud storage providers.

Cloud2Drive's striped virtual disk is similar to RAID 0, striping data across multiple cloud storage containers (from the same or different providers). Once data has been encrypted and obfuscated by Extenua's data protection algorithm, each individual slice of data is written to a different container. Data transfers to and from cloud storage containers aggregate the bandwidth among all storage containers for performance. An additional benefit is increased security, as a malicious actor gaining access to the administrator account of a single cloud storage provider cannot reconstruct the contents of a file.

Cloud2Drive's mirrored virtual disk is similar to RAID 1, where a copy of each file is written to all cloud storage containers (from the same or different providers), providing redundancy and ensuring data availability should communications to a cloud storage provider fail. Using mirroring, administrators can migrate data from one cloud storage provider to another.

Figure 8. Extenua Cloud2Drive Scalability



The amount of real storage represented by the virtual drive using aggregated cloud storage containers can be increased on the fly by adding storage containers to the virtual disk configuration. This enables organizations to scale their storage by purchasing additional capacity from cloud storage vendors, add the new storage containers to virtual disks, and instantaneously make that capacity available to users.

The cloud storage space is presented to the end-user through a virtual disk. Since operating systems need to know the available storage space, virtual disks must be configured with a size. The size presented to the OS is arbitrary, and can be changed at any time. A virtual disk that represented 1TB of storage can be instantly resized to 1PB.

ESG Lab tested the scalability of Cloud2Drive by adding storage containers to an existing virtual disk configured as a striped virtual disk. Using Cloud2Drive manager, ESG Lab changed the size of a virtual disk from 2GB to 20GB. Next, we logged out from Cloud2Drive, and logged back in. The virtual disk size as reported by Windows showed the new size of 20GB. End-user operation continued uninterrupted, and ESG Lab was immediately able to store additional data.

Why This Matters

The promise of enterprise file sync and share solutions is always on, always available, infinitely scalable data storage. Scalability and resiliency are crucial to maintaining an effective EFSS solution. By eliminating single points of failure, uptime requirements can easily meet customer requirements, ensuring data availability. Likewise, providing infinite storage capacity ensures that end-users and administrators are never stymied by running out of space during critical operations.

ESG Lab confirmed that Extenua Cloud2Drive could leverage multiple cloud storage providers to eliminate single points of failure, providing a highly available and redundant EFSS solution. Additionally, using mirrored backend cloud storage containers, data can be quickly and easily migrated from one provider to another. We validated Cloud2Drive's scalability by adding storage containers to virtual disks, increasing total storage capacity without disruption to users.

Artificial Intelligence Learning Engine for Local Caching

Most enterprise file sync and share solutions cache data on the local disk to provide users the ability to work even when connectivity to the cloud is lost. A problem arises when the cache grows large enough to consume all available local disk space, an especially critical challenge for mobile devices with limited local storage. Some EFSS solutions manage the cache automatically, while other solutions give control over the cache to the user.

Cloud2Drive automatically manages the local cache. However, instead of using the traditional cache control algorithm, which automatically deletes the least recently used files (LRU), Cloud2Drive incorporates an artificial intelligence learning engine to optimize the cache individually for each user. The AI engine learns user behavior in order to predict which files the user needs, taking into account many factors such as file similarities, file locations, and user actions.

Extenua designed the AI learning engine to run on both low-powered mobile devices and high-powered workstations. The AI engine uses two separate, lightweight AI learning algorithms, one more suited to stable behavior patterns, and one more suited to variable behavior patterns. Combining the results of both algorithms ensures that the AI engine can provide advantages for the widest variety of users and user behaviors.

Upon installation, the AI engine has no knowledge of the user’s behavior. During the initial learning phase, which typically takes a month, Cloud2Drive uses the traditional LRU algorithm to control the cache. Once the AI engine has developed enough knowledge about user behavior to intelligently control the cache, Cloud2Drive automatically switches from LRU to the AI engine. According to Extenua, the AI engine predicts the file needs of the user with 99% accuracy.

Why This Matters

The modern workforce depends on having continuous access to corporate data from anywhere using any device. When using enterprise file sync and share solutions, which provide users access to large and infinitely scalable pools of online storage, users need a local copy of their data to maintain productivity when connectivity is lost.

Extenua included an artificial intelligence learning engine in Cloud2Drive. The AI engine learns users’ behaviors, and caches critical files to local storage. According to Extenua, the AI engine is 99% accurate in predicting which files the user needs. Automatic local caching of files eliminates the time and effort of users actively managing which files are locally stored, and reduces expensive mobile data usage and charges to fetch forgotten files from the cloud. With Cloud2Drive, users have access to the correct set of files, whether they’re using mobile devices with limited local storage, or they’re disconnected from the network, and enables employees to embrace the work anytime, from anywhere, using any device paradigm.

The Bigger Truth

Security breaches are becoming a very common occurrence. Smartphones, tablets, Windows desktops, application servers, and infrastructure-as-a-service providers are all susceptible. Attacks affect both small and large organizations indiscriminately. The consequences can be devastating to operations, company reputations, and bank accounts, and the costs may include not just resuming operations and addressing security gaps, but legal liability and regulatory fines that can be a tremendous burden as well.

This may be why information security has remained at the top of the IT priority list for the last three years, according to ESG research. When asked to consider their organizations' most important IT priorities for 2015, information security initiatives were the most often cited, identified by 34% of respondents.[3]

The promise of enterprise file sync and share solutions is always on, always available and infinitely scalable data storage. However, achieving this promise should not come at the expense of data security. ESG Lab found that Extenua's Cloud2Drive EFSS solution includes heavyweight security, and is easy to understand and manage.

Cloud2Drive's heavyweight security scheme encrypts and obfuscates data at rest on the local disk, on the fly, and at rest at the cloud storage provider. The data obfuscation combined with encryption makes cracking very hard—it would take 25 eons to crack using all currently available computing power, according to Extenua. Deploying Cloud2Drive brings compliance with all security mandates in PCI DSS, HIPAA, CASB1386, GLBA, DoD 5015.2 and other regulations, and brings peace of mind to the security-conscious organization.

Cloud2Drive enables administrators to pool cloud storage from the same or different storage providers into virtual disks. Pooled storage provides security, performance, and redundancy while eliminating single points of failure, which enhances reliability and availability. Cloud2Drive achieves virtually unlimited scalability by adding cloud storage containers to the virtual disk storage pool.

The Cloud2Drive client software for Windows, Android, and iOS presents each virtual disk as a local disk. Users interact with the online storage the exact same way they interact with local storage. This makes it easy for administrators to rapidly deploy Cloud2Drive company-wide without having to train users, and provides an incentive for users to abandon insecure public online file sharing solutions.

Extenua's Cloud2Drive offers the features, capabilities, scalability and security that can satisfy organizations' requirements for data security and always on, always available, scalable enterprise file sync and share solutions. The ease of deploying, configuring, and maintaining Cloud2Drive, combined with extensive security, ensures that system administrators devote less time managing EFSS, freeing resources to address other critical parts of the IT infrastructure. Cloud2Drive supports the Windows platform, and Android and iOS mobile devices, and ESG Lab believes that support for the Macintosh platform would enable Cloud2Drive to reach a greater audience. Any business looking for a flexible, efficient EFSS solution to improve its data security while providing universal access to corporate data would be well-served by giving Extenua Cloud2Drive serious consideration.

[3] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.