EndPoint Device Secures Files Transferring and Sharing

1/24/2014 Rev 2.10

LucidPort Technology, Inc.

www.lucidport.com

Seminar series: Files transferring and Sharing

LucidPORT

Increasing Need for Data Protection

"Data breaches in the UK have increased tenfold in the past five years, figures from the Information Commissioner's Office (ICO) reveal." - BBC New Technology

Lax data protection practices will not be tolerated – ICO.

2012 -2013 £2.6 million in fines

Average fine is £130,000

Increasing Need for Data Protection (2)

> “The regulation, currently being debated in Brussels, will include stipulations to report data breaches within 24 hours of discovering them and fines of up to two percent of company turnover.”– Tech week Europe

“Room recommended those organisations worried about this tougher regulatory environment focus less on general compliance and more on securing private personal data, as that is where their reputation is maintained or destroyed.”

“When it comes to looking at regulatory pain, financial penalties, business needs to rebalance the focus away from general compliance issues, towards the security and confidentiality arenas. Too much energy has been focused on the wider compliance agenda. If you’re going to be driven by sanctions and bad publicity, you should re-focus towards security and confidentiality.”

Ref:

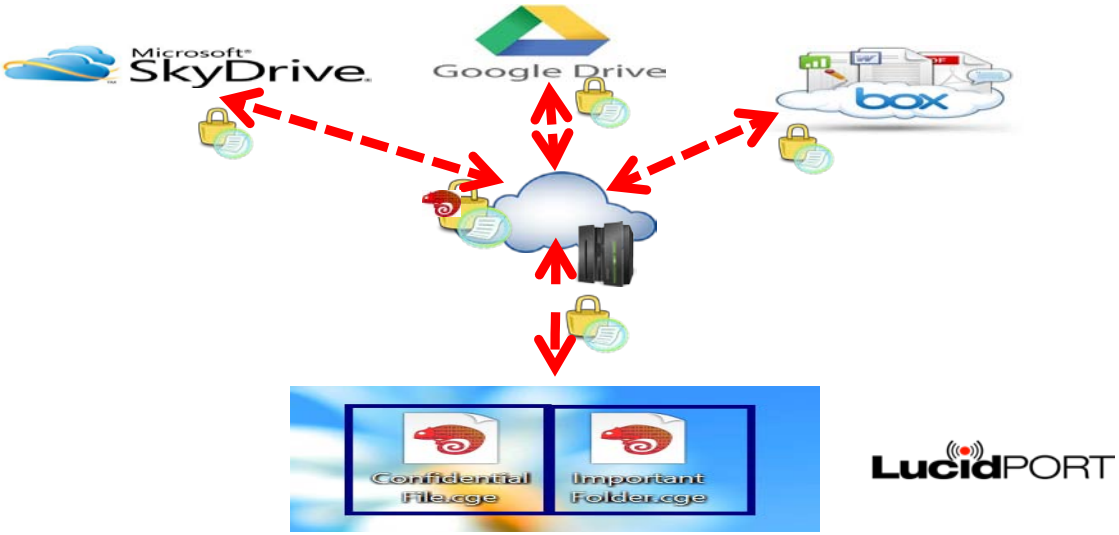
Lawyer: EU Privacy Laws Will Lead To Fining Frenzy In UK – Tech Week Europe; On January 21, 2014 by Tom Brewster

Who is reading your emails and files?

- Your company
- Your government
- Hackers
  - Supported by Government
  - Individual hackers for money
  - Originations are wishing to demonstrate. No motive for money

File transferring or sharing inside and outside of your company

- Email – Gmail, Hotmail, Yahoo Mail
- Cloud – Box, Google Drive, SkyDrive
- FTP site



Why employees use public networks and personal emails?

- No secure technical solutions provided
  - Lack of training
  - Management has no policy
- Easy to use, simple
- Files size is getting bigger
- Increase productivity

Problems with public networks and personal email

- Employees are using personal email to send sensitive files
  - Limited email attachment
- Employees are using cloud-based services to upload sensitive files

Cloud Storage Applications:

- Store files on Cloud storage
  - Where?
  - Who can access?
  - Legal rights?
- Share files
  - Who can share/read files?
  - Who can edit/write files?
- Issues

Scope of Security:

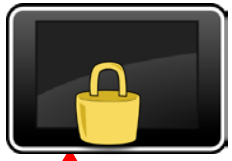
Internet, Cloud Computing and Computers

1. Web Security – Server security
2. Perimeter Security
3. Enterprise Computing Security – Server security
4. End user Security – Endpoint data protection
    - **in-use** (endpoint actions)
    - **in-motion** (network traffic)
    - **at-rest** (data storage)

- Cloud computing/storage adds more risk factors
- Security issues can be addressed.
- EndPoint Device is the solution for End user security.

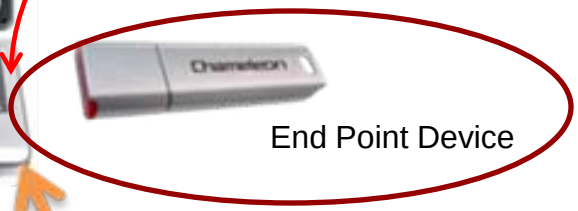
•bank account information
•driver license numbers
•social security numbers
•employee records

Win8 Tablet



Chameleon Secures Win8 Tablet

USB to USB Host cable for files sharing/transfer



End Point Device

GoogleDrive

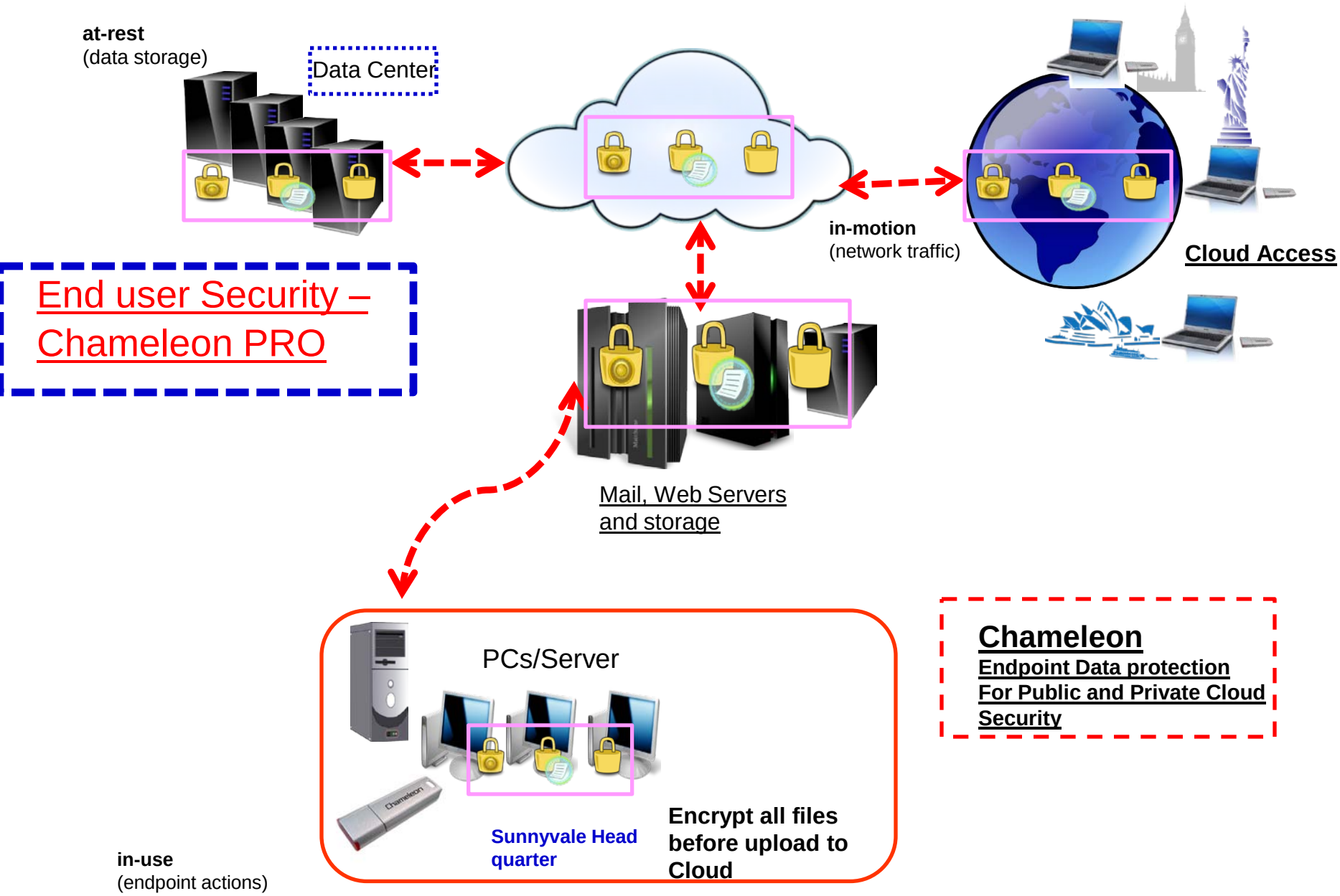
Box

Office 365

EndPoint (Chameleon) Deivce Secures All

•customers and patient information
•Movies
•Pictures
•Company IPs

Data on laptop and cloud: Bad thing will happen
– Dr. Ken Baylor


at-rest
(data storage)
Data Center
in-motion
(network traffic)
Cloud Access
End user Security –
Chameleon PRO
Mail, Web Servers
and storage
PCs/Server
Chameleon
Sunnyvale Head
quarter
Encrypt all files
before upload to
Cloud
in-use
(endpoint actions)
Chameleon
Endpoint Data protection
For Public and Private Cloud
Security

Criteria of Endpoint devices selection for End User Computing

- Capable to secure data
  - **in-use** (endpoint actions)
  - **in-motion** (network traffic)
  - **at-rest** (data storage)
- Who owns the device's source codes?
- Who owns the Master Key?
- Are there potential vulnerabilities/back door?
- Who manufactures the devices?
- Where is it manufactured?

Criteria of Endpoint devices selection for End User computing – (2)

- Easy installations, no need to call help desk
- No need to change computer current setup, no new commands and instructions to learn
  - Windows users don’t need any extra training
  - No conflict with existing installed security/data protection software, it adds security for existing monitor and recovery software
  - Strength End Point security
- Adds extra Security for Monitor, Recovery software with negligible cost
- Device performs cryptographic functions on behalf of the device owner
  - Encryption , Decryption ,Signing , Authentication

Requirements for a general purpose data protection device:

- Strong encryption
- Robust key management
- Usable anywhere
- Support multiple computers
- Secure any number of storage devices, including
  - Hard disks, internal or external
  - Flash drives
  - Files in cloud storage

Cloud Storage Privacy Issues

- Cloud Computing/Storage
  - Security issues
    - Private Cloud vs Public Cloud
    - Record Keeping Laws require data to stay local?
    - Cloud Service Providers' Data Centers and Systems for Auditing issues
  - Legal – Term and Service Agreements
  - USA Patriot Act
    - non- US companies gain Marketing Advantages
- Consumer Privacy Bill of Rights
  - Individual Control ,Transparency ,Respect for Context, Security, Access and Accuracy, Focused Collection, Accountability
  - with International Interoperability, Examples, APEC, US-EU Safe Harbor

Do you know where your data is?

Existing Solutions

- Software encryption (TrueCrypt, BitLocker, etc.)
  - Since the PC must know the encryption key, it can be attacked by hackers, spyware, key-loggers, and other software (like Kon-Boot)
  - Vulnerable to cold boot attacks (recover encryption key from RAM)
  - Yet another password that can be stolen without your knowledge
- Encrypted disks/ Thumb drives: Could add extra cost per disk/drive
  - You lose your data if the disk is lost or broken
  - Your backups are unencrypted. Backups can only be made with the drive unlocked.
  - Traces of your private files remain in the PC's hard drive
  - Limited capacity
  - Yet another password that can be stolen without your knowledge
- Software for cloud applications
  - Who owns the encryption Key and Master Keys
  - Can not share files in encrypted format
  - Where in the chain is the data actually encrypted (protected)?

Comparison of Encryption Technologies

	Software	Hardware : Encrypted Disks	Hardware : Chameleon (LucidPort)
Encryption Key Management	Complex	Drive provides single key	User controls encryption keys (easy and secure)
Costs	High: Continuing (upgrade) life cycle costs	Medium: Pro-rated into the initial drive cost	Low: Fixed at one time purchase cost
Migration or Re-Encryption	Complex	None	Easy
Installation and Use	Complex	None	Easy and secure
Supports multiple devices	Yes, new setup for each drive	Fixed, can only use for single drive	Supports multiple drives and devices

The Security risks of using Cloud Computing

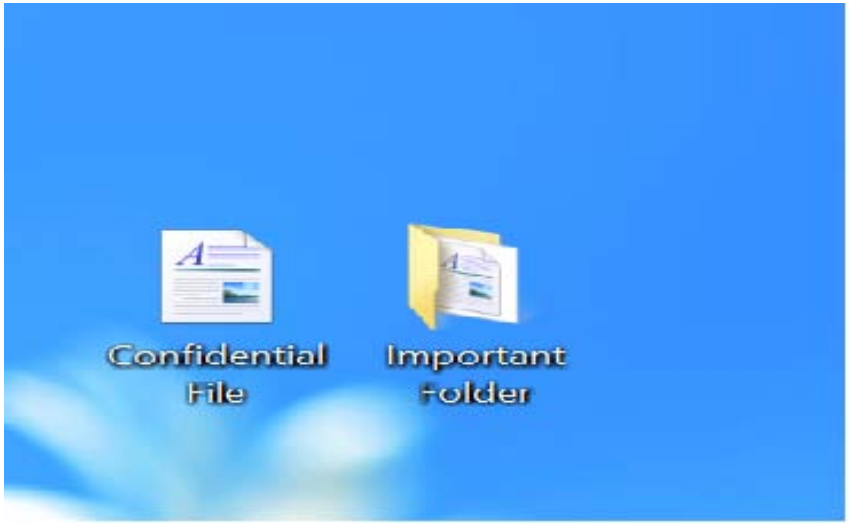
Security issues can be addressed.

- Where is your data stored and who can access your data?
- Data center security?
- Controls? – administration and management
  - **in-use** (endpoint actions)
  - **in-motion** (network traffic)
  - **at-rest** (data storage)
  - Key Management

- Chameleon PRO is the solution.

Example:
To upload and store encrypted file or folder to Cloud

A file, a group of files or folder that you want to store in cloud storage.



LucidPORT

Two steps to create encrypted file or folder

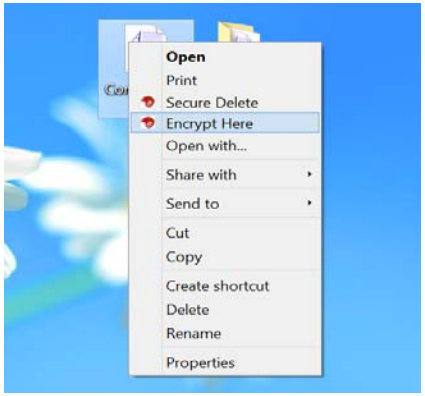
Step #1

Right click on the file or folder you want to protect

Step #2

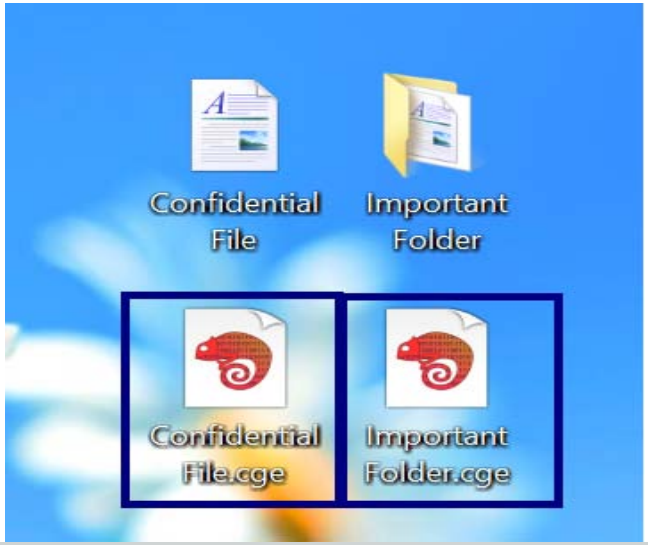
Select “ Encrypt Here” to

create an encrypted version of the selected file

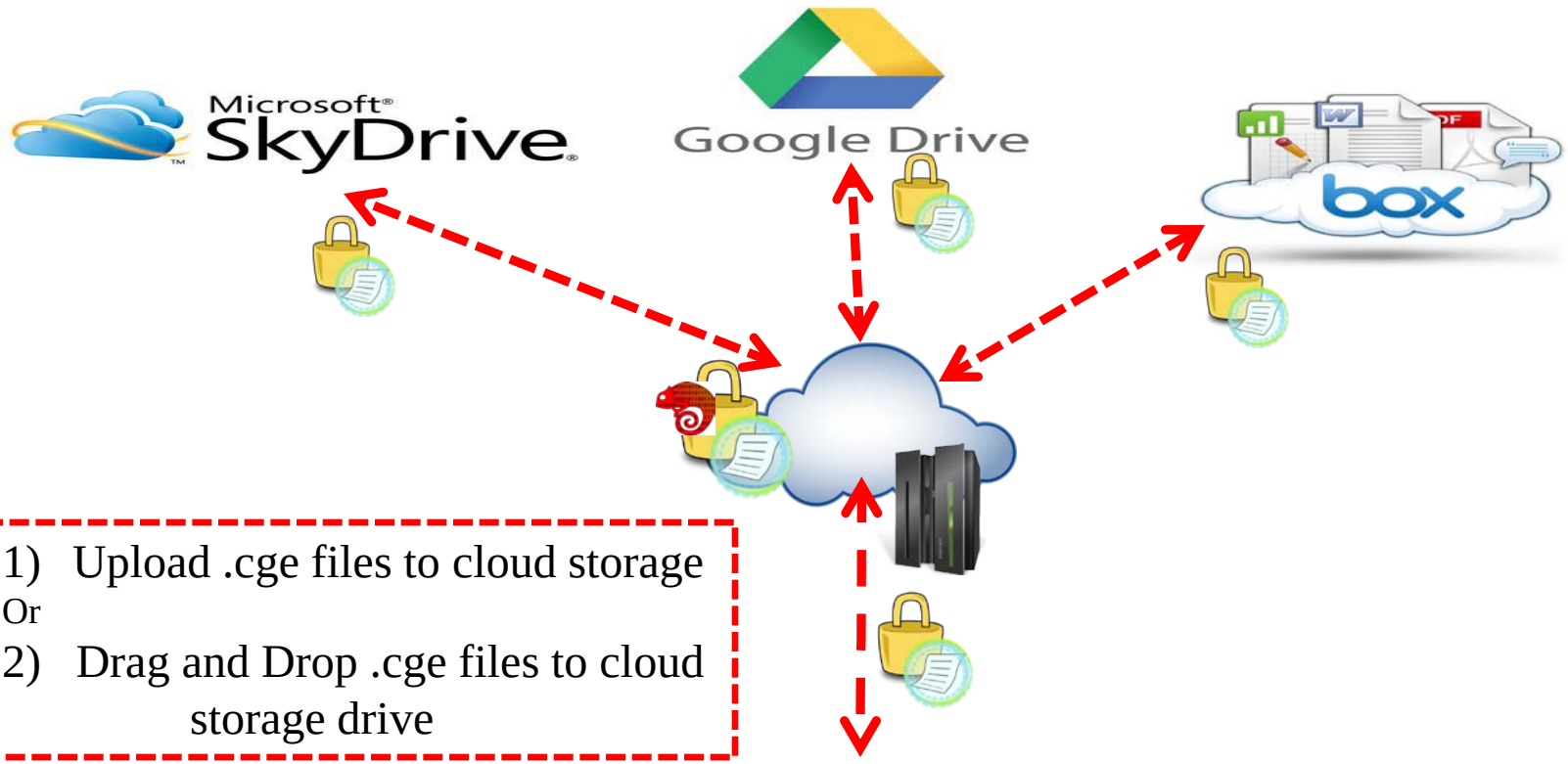


Two steps to create encrypted file or folder (2)

- The encrypted file or folder appears with the same file name but with the extension ".cge".
- To upload and store files with extension .cge to cloud



LucidPORT



1) Upload .cge files to cloud storage

Or

2) Drag and Drop .cge files to cloud storage drive

LucidPORT

Upload the encrypted .cge files to the cloud storage.

Data Protection Basic Guidelines

- Confidential information must be protected from unauthorized access or loss at all times.
  - Encrypt all information before upload to cloud or VPN
  - Do not send Password through email
- Information exists in three domains:
  - In-motion, at-rest, in-use
- Data “in-use” must be un-encrypted. In all other domains, confidential data should be encrypted.
- The Data Encryption Key (DEK) is the critical point of attack.

Data Protection Basic Guidelines (Conti.)

- Employees know to use computers.
- Blocks give employees incentives to defeat the blocks.
- Train employees about security.
- Give employees incentives to follow safe practices.
- Give clear policies for communicating with vendors and customers
- A personnel Endpoint Protection Device such as Chameleon makes it easy to manage Data Encryption keys and keep data safe.

Summary:

- Cloud storage adds security risks
  - IT provides technology for secure files
  - Management should have security policy in place, employees should observe the security policy
- Users should receive proper guidelines to handle security
  - Blocking and monitoring Cloud use is an expansive option
- Encrypt files/data before upload to cloud
- www.lucidport.com/chameleon

Tips: Chameleon keeps your sensitive files protected:

1. Use Chameleon to create an encrypted drive and store your sensitive files into encrypted drive.
2. Use Chameleon to create an encrypted drive on your external storage devices to store your sensitive files and keep your flash drive in a secure place.

   Or

   Chameleon encrypts files and store encrypted files into your removable media, such as flash drive and external hard drive and keep the drives in a secure place.
3. Use Chameleon's "Secure Delete" to erase sensitive files on your computer including external removable medias, such as portable hard drive and flash drive
4. Back up sensitive files to encrypted drive, sending only encrypt files to cloud or outside backup service.
5. Creating a Password.doc contains password , userID# and security question save Password.doc into encrypted drive, use Chameleon to encrypt Password.doc and Chameleon creates a new encrypted file called password.cge. Save password.cge to removable media and keep in a safe place.