EndPoint Device Secures Cloud Storage

WeiTi Liu and Reid Augustin

LucidPort Technology, Inc.

www.lucidport.com

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

Cloud Computing and Storage - Basic

- Cloud Computing and Cloud Storage
  - Application, Platform and Infrastructure
  - Hosting and files sharing
- Cloud Models
  - Public Cloud
  - Community Cloud
  - Hybrid Cloud
  - Private Cloud

Source:wikipedia.org

http://en.wikipedia.org/wiki/Cloud_computing

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

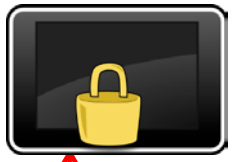
1. Web Security – Server security
2. Perimeter Security
3. Enterprise Computing Security – Server security
4. End user Security – Endpoint data protection
   - **in-use** (endpoint actions)
   - **in-motion** (network traffic)
   - **at-rest** (data storage)

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

Flash Memory SUMMIT

- 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

GoogleDrive

Box

Office 365

End Point Device

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

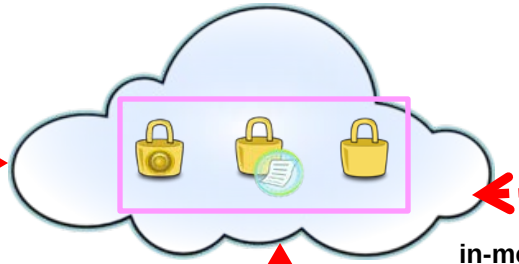
EndPoint (Chameleon) Device Secures All

Data on laptop and cloud: Bad things will happen

– Dr. Ken Baylor

at-rest
(data storage)

Data Center

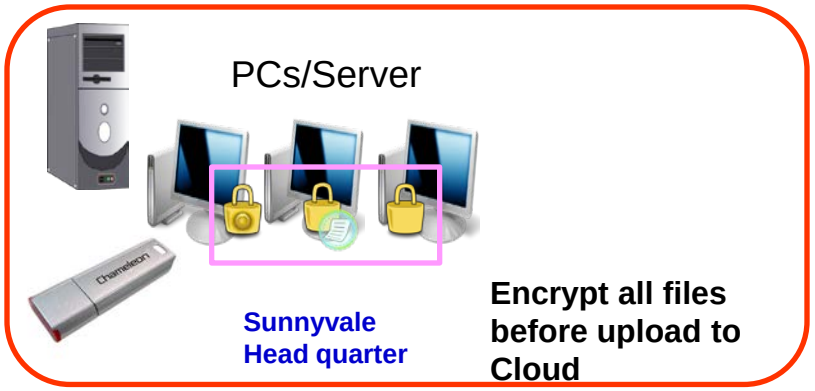


in-motion
(network traffic)

Cloud Access

End user Security – Chameleon PRO

Mail, Web Servers and storage



in-use
(endpoint actions)

Chameleon
Endpoint Data protection For Public and Private Cloud Security

Criteria of Endpoint devices selection for cloud storage

- Capable to secure data in-use, In-motion and at-reset
  - **in-use** (endpoint actions)
  - **in-motion** (network traffic)
  - **at-rest** (data storage)
- Who owns the device's source, and Master Key?
- Who owns the backdoor solutions?
- Who and where the devices are manufactured?
- A general purpose data protection device(Engine) with strong encryption can be used in anywhere,
  - supporting multiple computers
  - storage devices including external flash drive and hard disk
  - Cloud computing
  - secures unlimited numbers of storage devices

Criteria of Endpoint devices selection for cloud storage – (2)

- Easy installation, 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
  - Strengthen 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

Cloud Storage Privacy Issues

Do you know where your data is?

- 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
    In fact, it sounds that EU's new law forced US to establish this new law?

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
  - 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 clouds application
  - Who owns the encryption Key and Master Keys
  - Can not share files in encrypted format

Hardware encryption (Chameleon, Encrypted Disks) versus Software encryption

	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.

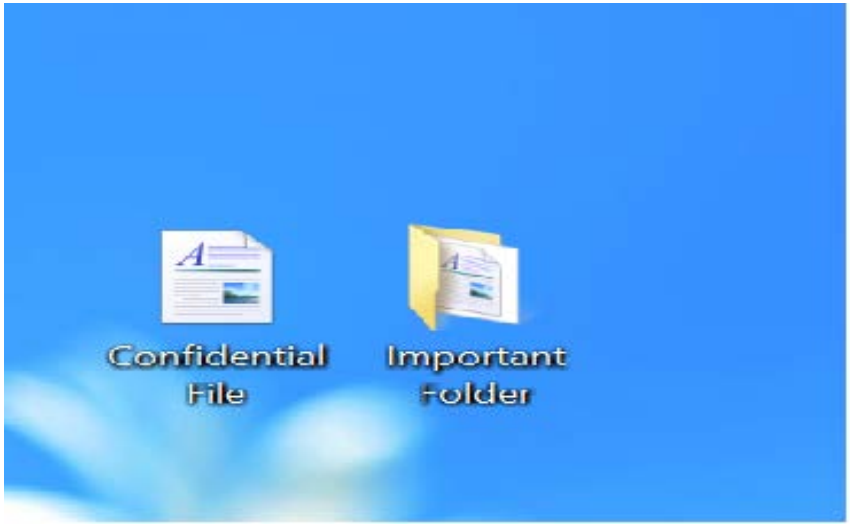
- Where is your data being stored and who can access to your data?
- Data center security?
- Protection of Data at rest?
  - Encrypted?
- Are data at rest and transit encrypted?
- Controls? – administration and management
  - **in-use** (endpoint actions)
  - **in-motion** (network traffic)
  - **at-rest** (data storage)

- Chameleon PRO is the solution.

Example:

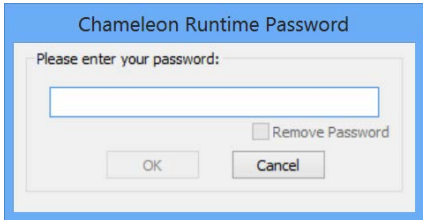
To use Chameleon to upload and store encrypted file or folder to Cloud

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



Two steps to create encrypted file or folder

Encrypting Files or Folders:



Plug in Chameleon Device

Enter your password (password enabled)

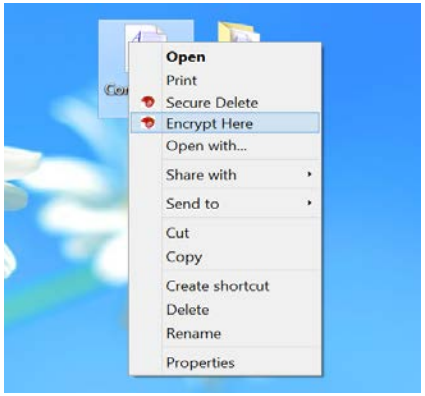
Step #1

Right click on the file or folder you want to protect

Step #2

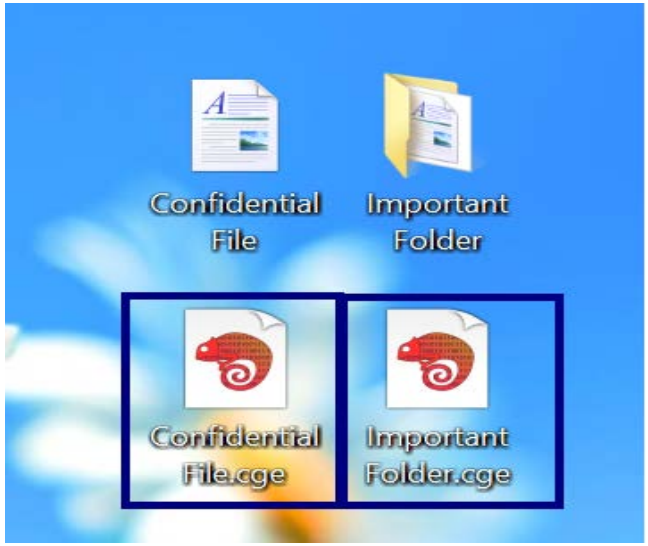
Select “ Encrypt Here” to

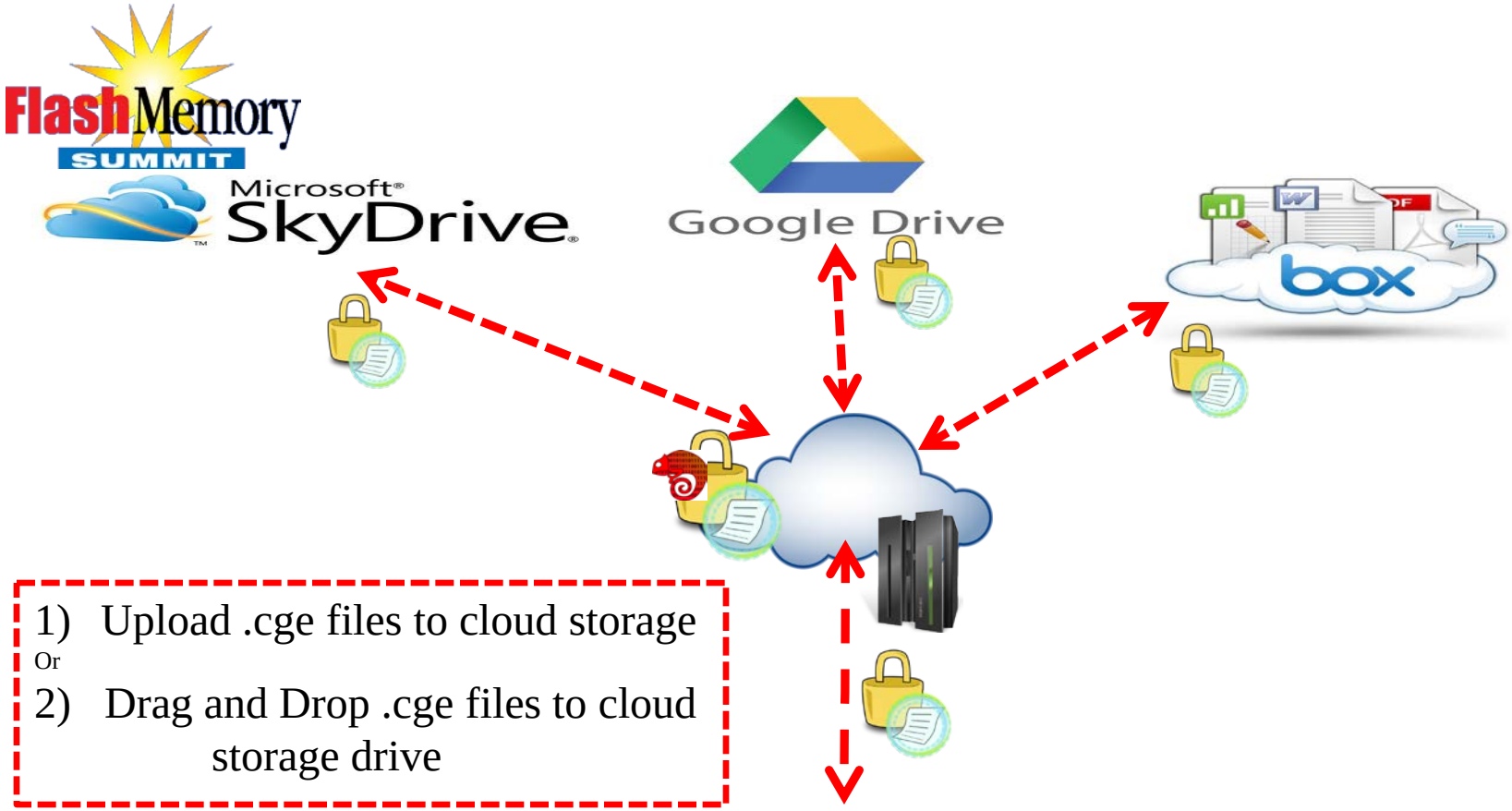
create an encrypted version of the selected file



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





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.

Note: For Cloud setup procedures, please refer to Cloud Providers Documentations

Data Protection Basic Guidelines

- Must secure confidential information at all times and to use End Point protection device to encrypt date to prevent unauthorized access or loss
  - Encrypt all information before upload to cloud or VPN
  - Do not send Password through email
  - In-motion, at-rest, in-use
- To protect information from unauthorized access, to save confidential information in encrypted formats
- Store confidential information in electronics with encryption
- Make sure your computers are password-protect, encrypt your files on computer

Data Protection Basic Guidelines (Conti.)

- Provide training to employees and Managements
  - Employees and managements know how to use computers.
  - Provide company security policy and guidelines
    - Do and Don’t
      - policy of using Flash Drives and Cloud
      - Blocking is not a solution.
      - How to communicate with your vendors and customers?
- LucidPort Chameleon provides Computer security and information security.

Flash Drive's role in Cloud computing world

- USB Flash drives are secure, when
  - store encrypted data/files on Flash Drive, not plain text files
- Back up

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 usage is an expansive option
- Encrypt files/data before upload to cloud
- www.lucidport.com/chameleon

All trademarks are the property of their respective owners.