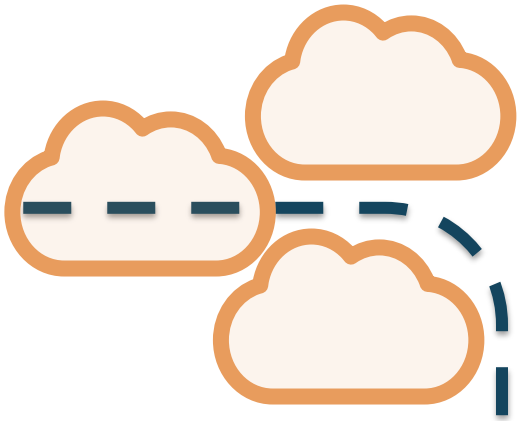
Facilitating Fluffy Forensics

Andrew Hay
~~Chief Evangelist~~
Director of Applied Security Research
andrew@cloudpassage.com

CloudPassage

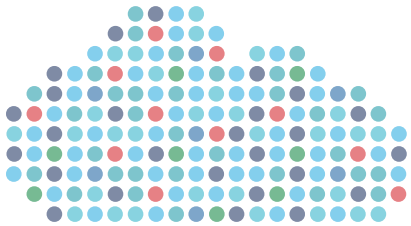
Overview



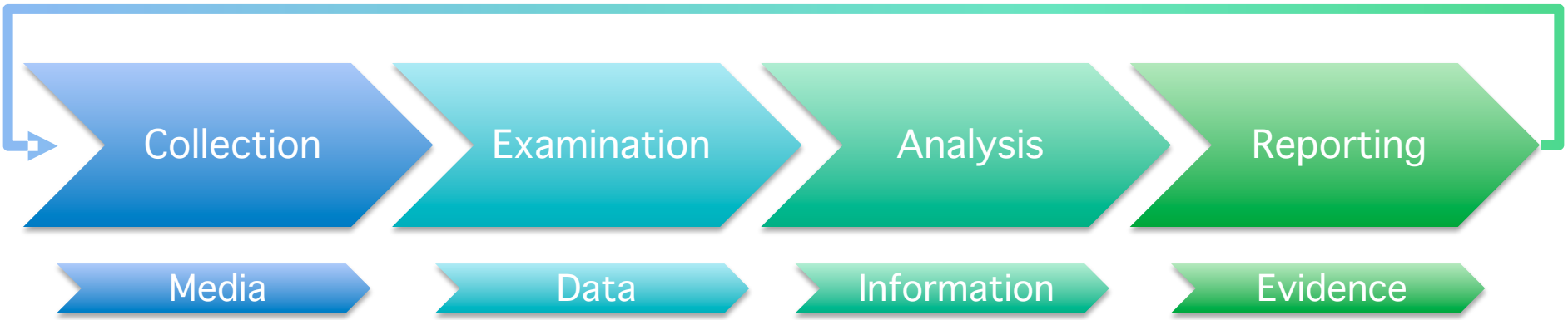
- Traditional forensics and IR
- Cloud architectural challenges for responders
- Legal issues and chain-of-custody
- How existing forensics/IR tools can help
  - and what they can do better
- Advantages of conducting forensics/IR in cloud environments

CloudPassage

Traditional Forensics and Incident Response



Forensic & Incident Response Process



NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response

CloudPassage

Simplified Definition

Source: http://en.wikipedia.org/wiki/Digital_forensic_process

CloudPassage

Acquisition: Images/Data

- **Physical partitions**
  - e.g. `/dev/hda` (first IDE physical drive)
- **Logical partitions**
  - e.g. `D:\`
  - e.g. /dev/hda2 (second logical partition)
- **Image files**
  - e.g. `/home/you/data.iso`
- **Contents of folder**
  - e.g. C:\Users\you*
  - Logical file-level analysis only
    - i.e. no deleted/unallocated files

CloudPassage

Analysis: Pieces of the Puzzle

- **SOFTWARE**
  - OS version
  - Installed applications list
  - Search history
- **SAM**
  - Last logged on user
  - Last failed logon
  - Username & SID
- **SYSTEM**
  - Shutdown
  - Time zone
  - Removable storage devices
- **NTUSER.DAT**
  - Drives mounted by user
  - File Ext Associations

CloudPassage

Analysis: Volatile Pieces

- **System**
  - Running processes
  - Scheduled jobs
  - Network connections
  - Memory
  - Logs
- **Users**
  - Currently logged in
  - Internet history
  - Environment variables
  - Browser data
  - Interaction

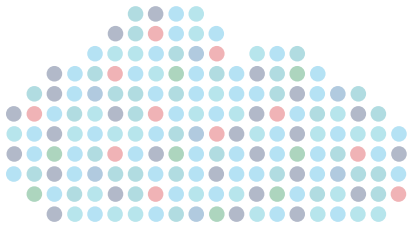
CloudPassage

Reporting: Tools

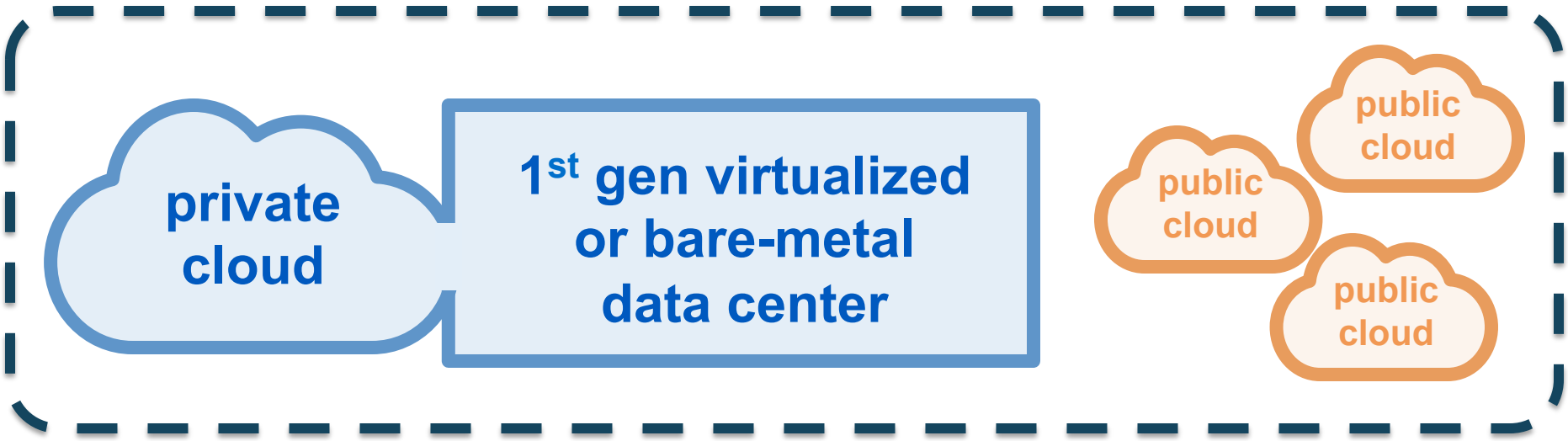
- **Enterprise forensics tools**
  - AccessData, Guidance Software, etc.
- **Open source tools**
  - SANS SIFT kit
- **Log management tools**
  - Splunk, SumoLogic, etc.
- **Poor people tools**
  - vi, notepad, MS Excel, etc.

CloudPassage

Cloud Architectural Challenges For Responders



Cloud Architectures

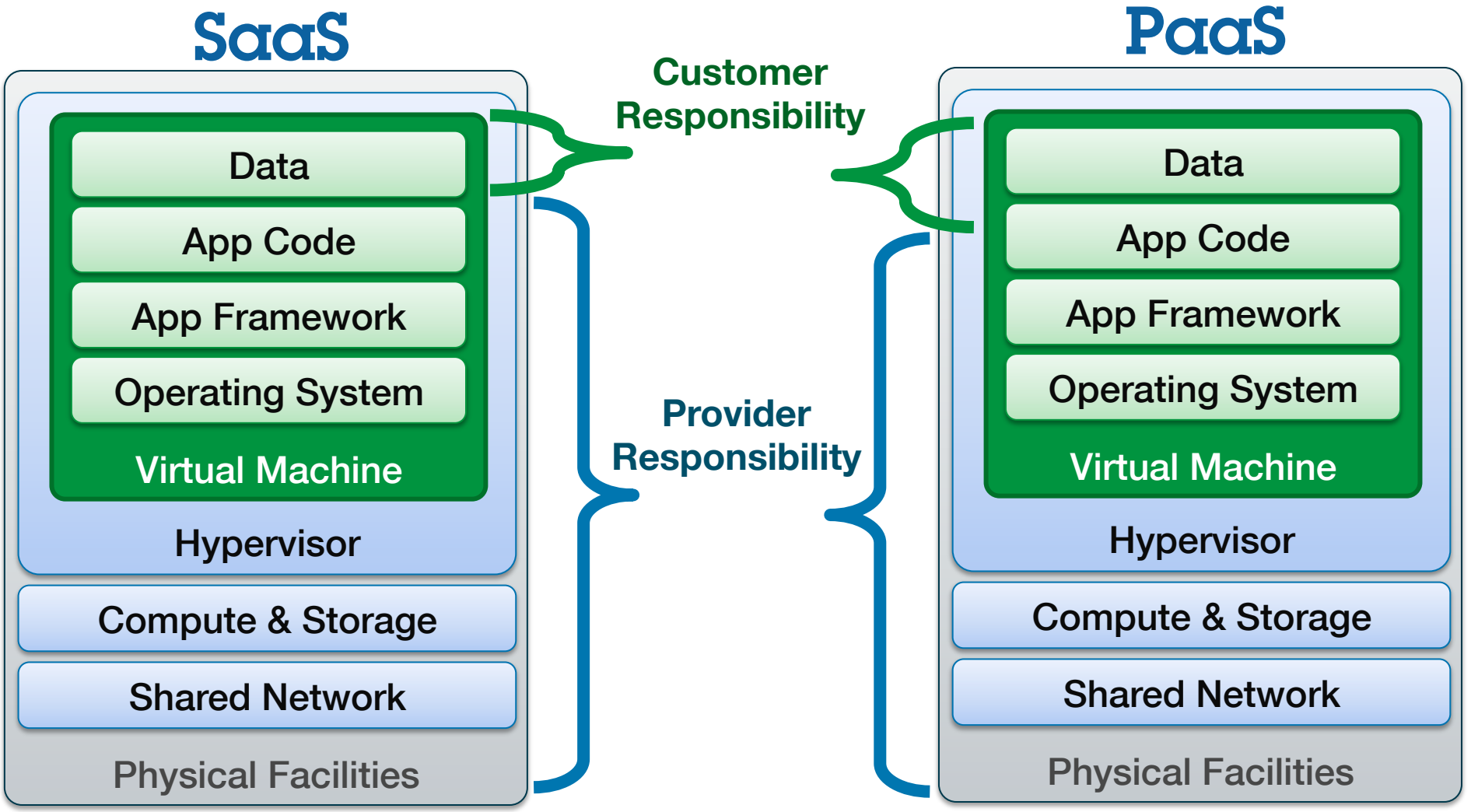


Cloud means many things to many people

- Private, public, or hybrid?
- SaaS, PaaS, or IaaS?
- On-prem, off-site, hosted?
- Single tenant, multi-tenant?

CloudPassage

Cloud Security Responsibility



CloudPassage

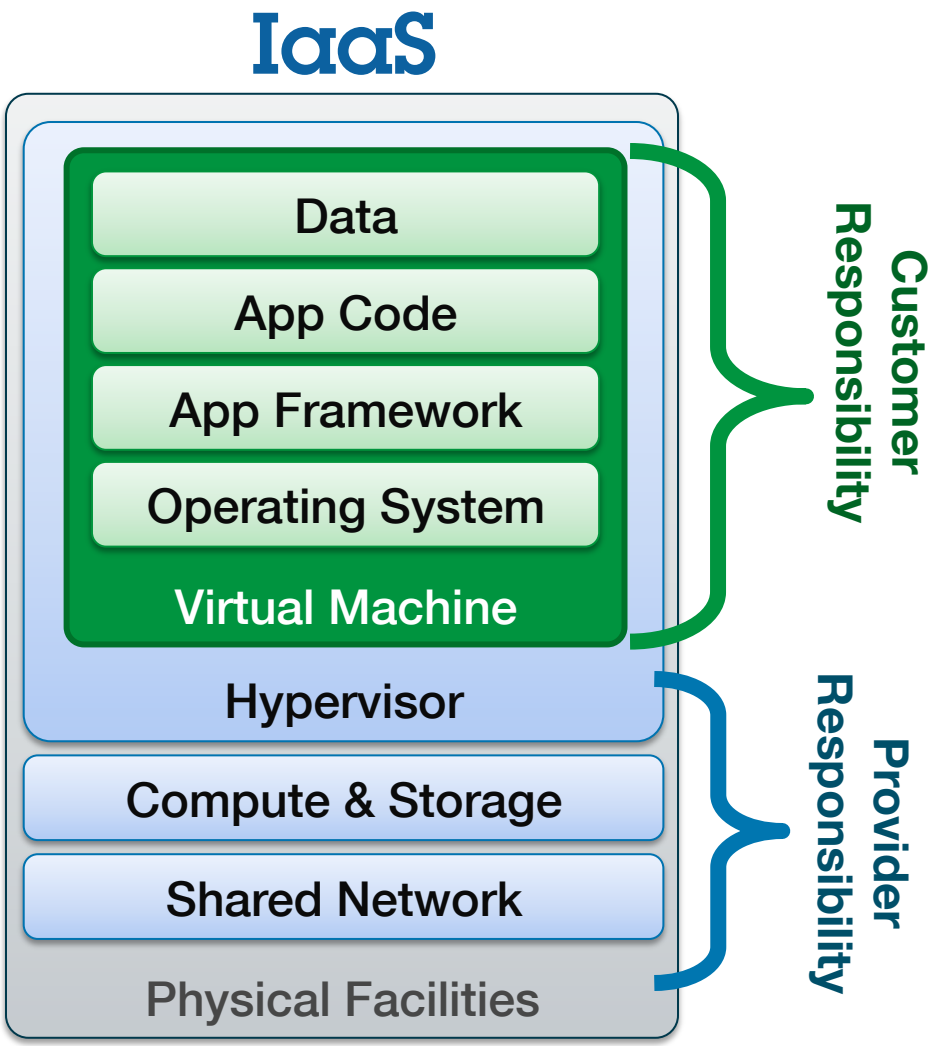
Cloud Security Responsibility

AWS Shared Responsibility Model

"…the **customer should assume responsibility and management** of, but not limited to, the guest operating system…and associated application software..."

"it is possible for customers to **enhance security** and/or meet more stringent compliance requirements **with the addition of… host based firewalls, host based intrusion detection/prevention**, encryption and key management."

Amazon Web Services: Overview of Security Processes



CloudPassage

5 Major Challenges

- Data residence
- Physical acquisition
- Instance isolation
- Hypervisor introspection & data integrity
- Lack of CSP collaboration/support

CloudPassage

Data Residence

- Need to know where the data is
- This adds validity to your investigation
- This, in turn, makes your results more credible

CloudPassage

Data Residence: AWS

Q: Where is my data stored?

Amazon S3 offers storage in the US Standard, US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), South America (Sao Paulo), and AWS GovCloud (US) Regions. You specify a Region when you create your Amazon S3 bucket. Within that Region, your objects are redundantly stored on multiple devices across multiple facilities.

Source: http://aws.amazon.com/s3/faqs/#Where_is_my_data_stored

CloudPassage

Data Residence: Windows Azure

Location of Customer Data

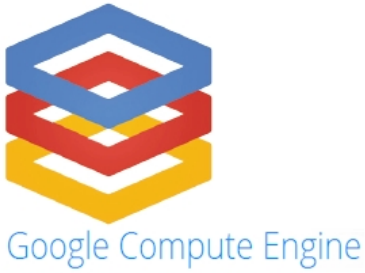
Windows Azure™

Microsoft may transfer Customer Data within a major geographic region (e.g., within Europe) for data redundancy or other purposes. For example, Windows Azure Storage geo-replication feature will replicate Windows Azure Blob and Table data, at no additional cost, between two sub-regions within the same major region for enhanced data durability in case of a major data center disaster. However, customers can choose to disable this feature.

Source: http://www.windowsazure.com/en-us/support/trust-center/privacy/

CloudPassage

Data Residence: GCE



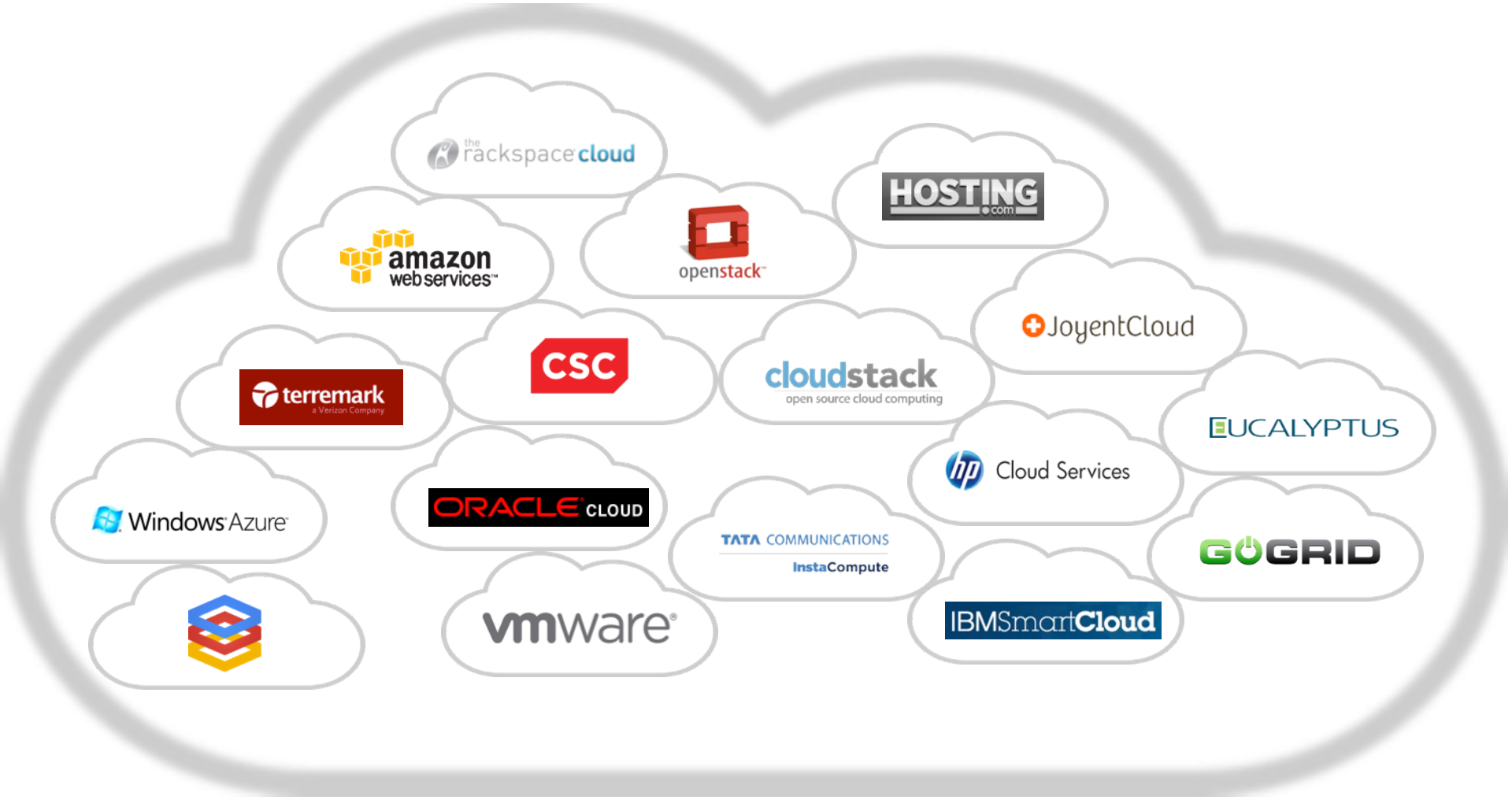
Q: Do I have the option of using a regional data center in selected countries?

Yes, Google Compute Engine offers datacenter options in Europe and within the United States. These datacenter options are designed to provide low latency connectivity options from those regions, however **at this time selection of datacenter will make no guarantee that project data at rest is kept only in that region**.

Source: https://developers.google.com/compute/docs/faq#zones

CloudPassage

Multi-Cloud Data Residence?



CloudPassage

Catching Clouds is Hard Work

CloudPassage


Catching a Specific Cloud is Harder

Physical Acquisition

- Unless you own the cloud architecture…
- Or have the bent the CSP to your will…
- You may be stuck with snapshots and/or logical imaging

CloudPassage

Image Acquisition: AWS

- There are 3 ways that I know of
  1. Snapshot the EBS volume, mount, and copy locally
  2. Have AWS ship you the data from S3 on physical device
  3. Use AMI Tools to compress, encrypt, and sign a snapshot

Image Acquisition: AWS EBS

- Launch a clean Amazon Linux AMI
- Stop the instance of the root volume you wish to capture
- Detach the `/dev/sda1` volume
- Create a snapshot of the now detached `/dev/sda1` volume
- Attach the `/dev/sda1` volume to the new AMI as `/dev/sdf` (don't mount)

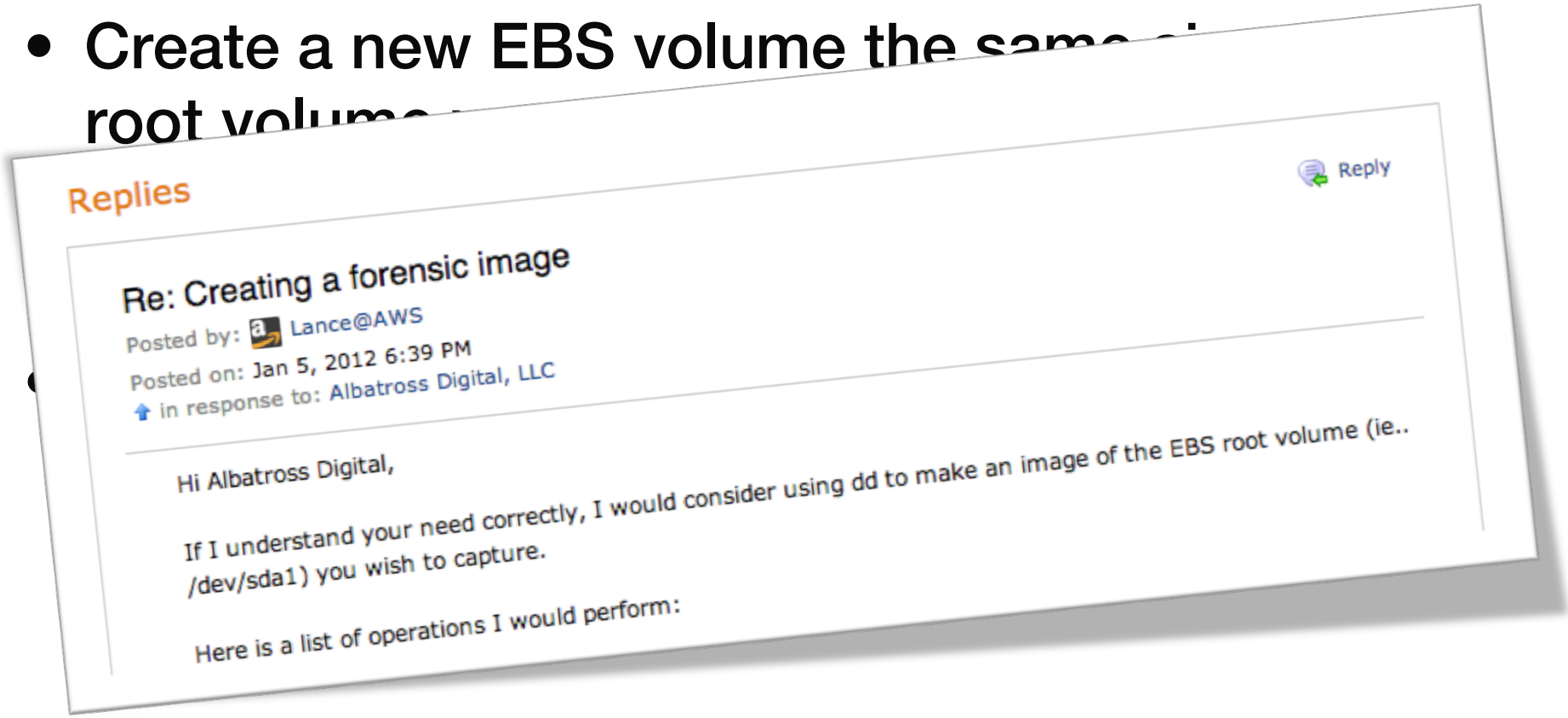
Image Acquisition: AWS EBS

- Create a new EBS volume the same size as the root volume you wish to capture
- Attach this new volume as `/dev/sdg`
- Then use these commands:
  - sudo mkfs -t ext3 /dev/sdg
  - sudo mkdir /vol1
  - sudo mount /dev/sdg /vol1
  - sudo chown ec2-user /vol1
- Use dd to make an image of /dev/sdf
  - `sudo dd if=/dev/sdf | gzip -c > /vol1/sda1.img.gz`

CloudPassage

Image Acquisition: AWS EBS

- Create a new EBS volume the same size as the root volume



Replies

Reply

Re: Creating a forensic image

Posted by: Lance@AWS

Posted on: Jan 5, 2012 6:39 PM

in response to: Albatross Digital, LLC

Hi Albatross Digital,

If I understand your need correctly, I would consider using dd to make an image of the EBS root volume (ie.. /dev/sda1) you wish to capture.

Here is a list of operations I would perform:

- Use dd to make an image of /dev/sdf
  - `sudo dd if=/dev/sdf | gzip -c > /vol1/sda1.img.gz`

CloudPassage

Image Acquisition: AWS S3

- Amazon provides a service to export data from S3 onto a physical device and ship it to the requestor
- Customer must provide the storage device and is billed $80 per storage device handled plus $2.49 per data-loading hour
- In EBS or S3 methods it is impossible to verify the integrity of the forensic disk image*

Source: J. Dykstra, A.T. Sherman / Digital Investigation 9 (2012) S90–S98

CloudPassage

Image Acquisition: AWS S3 + AMI Tools

- **ec2-bundle-vol**
  - Creates a bundled AMI by compressing, encrypting and signing a snapshot of the local machine's root file system
- **ec2-migrate-bundle**
  - Copies a bundled AMI from one Region to another
- **ec2-download-bundle**
  - Downloads the specified bundles from S3 storage

Dykstra/Sherman Experiment

- **Experiment by J. Dykstra, A.T. Sherman**
  1. Manual installation of EnCase Servlet and FTK Agent
  2. Used VM introspection for complete drive image
  3. AWS Export process (ship a drive)

Experiment	Tool	Evidence collected	Time (hrs)	Trust required
1	EnCase	Success	12	OS, HV, Host, Hardware, Network
1	FTK	Success	12	OS, HV, Host, Hardware, Network
1	FTK Imager (disk)	Success	12	OS, HV, Host, Hardware, Network
1	Fastdump	Success	2	OS, HV, Host, Hardware, Network
1	Memoryze	Success	2	OS, HV, Host, Hardware, Network
1	FTK Imager (memory)	Success	2	OS, HV, Host, Hardware, Network
1	Volume Block Copy	Success	14	OS (imaging machine), HV, Host, Hardware, Network
2	Agent Injection	Success	1	HV, Host, Hardware, Network
3	AWS Export	Success	120	AWS Technician, Technician's Host, Hardware and Software, AWS Hardware, AWS Software

Source: J. Dykstra, A.T. Sherman / Digital Investigation 9 (2012) S90–S98

CloudPassage

Closer Look…

Experiment	Tool	Evidence collected	Time (hrs)
1	EnCase	Success	12
1	FTK	Success	12
1	FTK Imager (disk)	Success	12
1	Fastdump	Success	2
1	Memoryze	Success	2
1	FTK Imager (memory)	Success	2
1	Volume Block Copy	Success	14
2	Agent Injection	Success	1
3	AWS Export	Success	120

Closer Look…

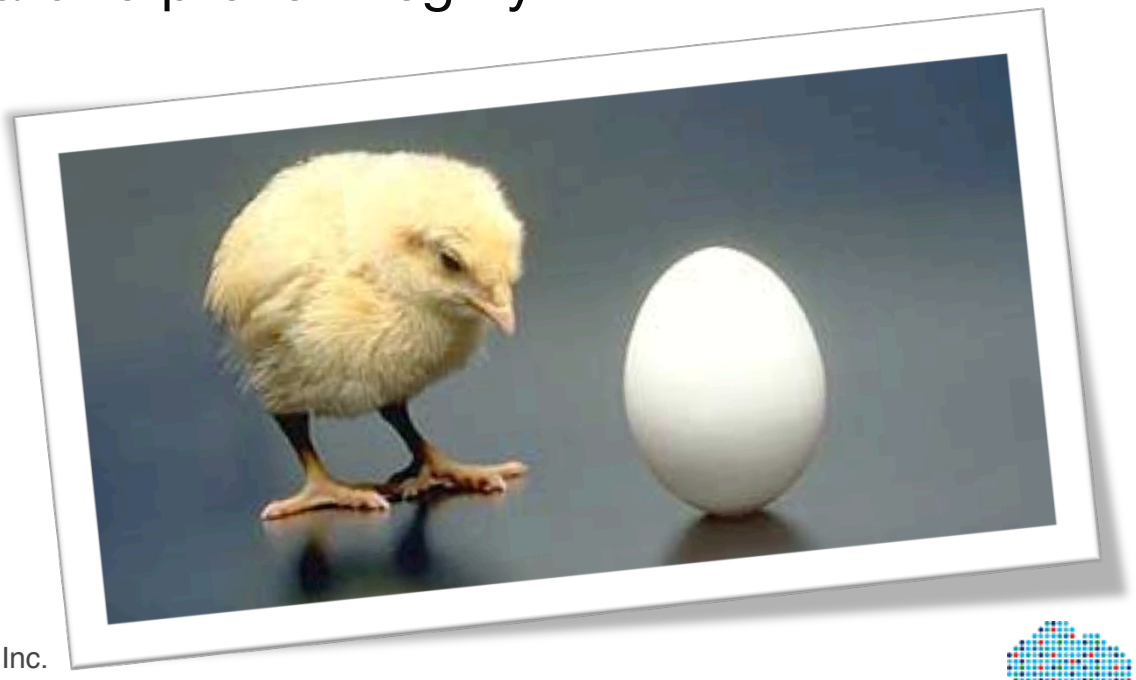
Experiment	Trust required	Time (hrs)
1	OS, HV, Host, Hardware, Network	12
1	OS, HV, Host, Hardware, Network	12
1	OS, HV, Host, Hardware, Network	12
1	OS, HV, Host, Hardware, Network	2
1	OS, HV, Host, Hardware, Network	2
1	OS, HV, Host, Hardware, Network	2
1	OS (imaging machine), HV, Host, Hardware, Network	14
2	HV, Host, Hardware, Network	1
3	AWS Technician, Technician's Host, Hardware and Software, AWS Hardware, AWS Software	120

Introspection & Data Integrity

- **Introspection is not new**
  - First introduced by T. Garfinkel and M. Rosenblum in *A Virtual Machine Introspection Based Architecture for Intrusion Detection*
- **Way to look into current state of the guest virtual machine**
  - e.g. covert, low-level access to read find processes and threads, recover files mapped in memory, and extract information about the Windows registry

Introspection & Data Integrity

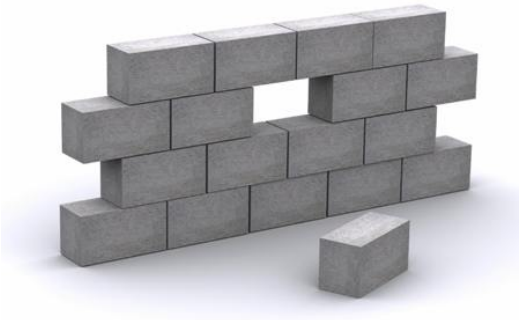
- Enabled by provider
- Transparent to tenant and server instance
- Great for forensic acquisition
  - but hard to prove integrity



CloudPassage

Instance Isolation

- **Several conditions must be met in order for a cloud instance to be successfully isolated:**
  - **Location:** The physical location of the instance is known
  - **Incoming & Outgoing Blocking:** The instance is blocked from sending/receiving communications to/from the outside world



Source: Waldo Delport and Martin Olivier - *Isolating Instances In Cloud Forensics*

CloudPassage

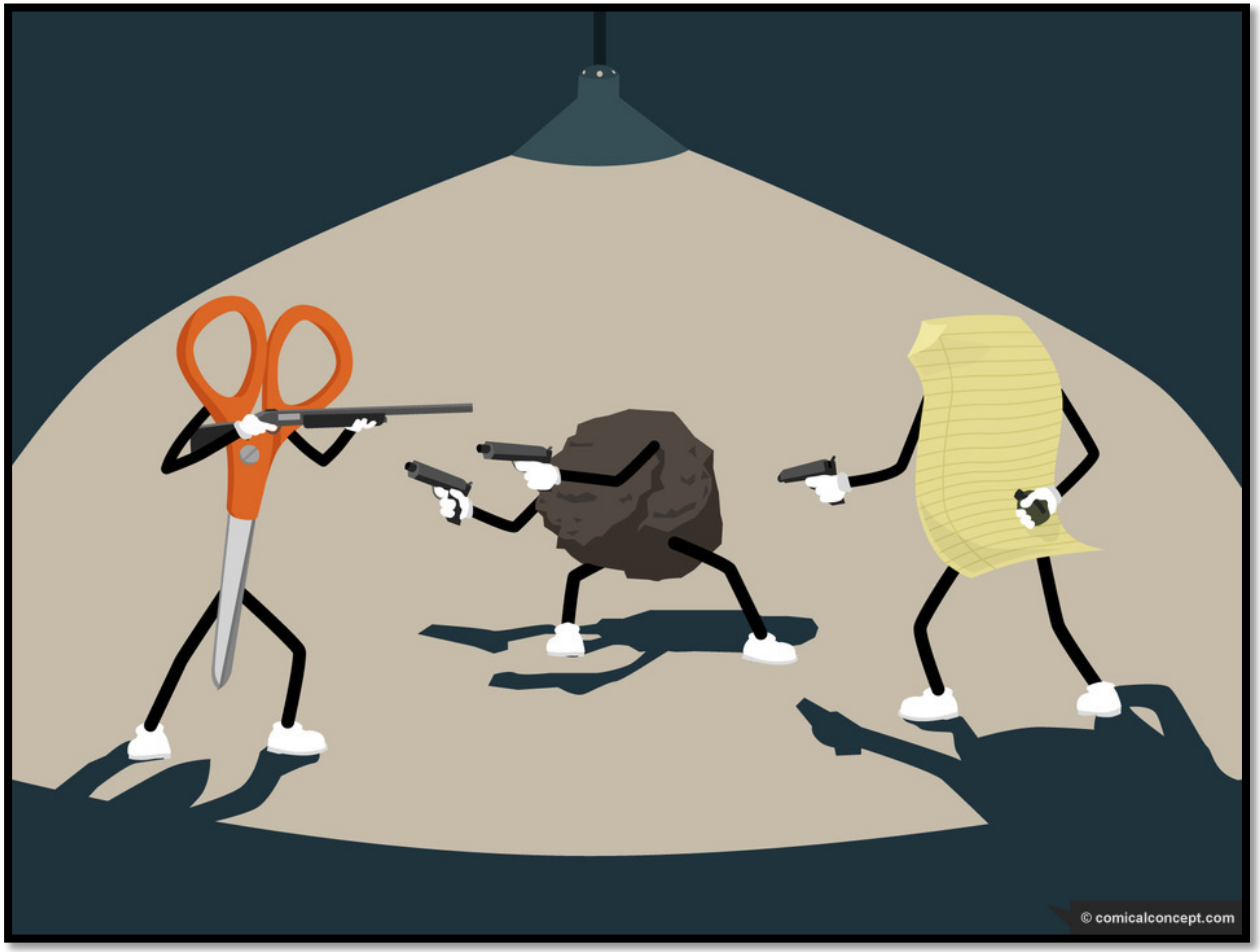
Instance Isolation

- **Several conditions must be met in order for a cloud instance to be successfully isolated:**
  - **Collection:** Evidence from the instance can be gathered
  - **Non-Contamination:** Evidence from the instance is not contaminated by the isolation process
  - **Separation:** Information unrelated to the incident is not part of the isolation process

Source: Waldo Delport and Martin Olivier - *Isolating Instances In Cloud Forensics*

CloudPassage

CSP Collaboration/Support



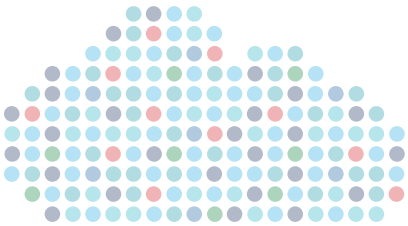
CloudPassage

CSP Collaboration/Support

- Most providers have people that can help
- Contracts should indicate level of effort…
  - That you're expected to exert
  - That they're willing to exert
- Ask for:
  - Samples/examples of past investigations
  - Methodologies employed
  - Credentials of staff
  - Interviews with CSP team members

CloudPassage

Legal Issues



Legal Issues: I am not a lawyer

- I'm Canadian…

CloudPassage

Legal Issues: I am not a lawyer

- Our lawyers wear funny wigs…

CloudPassage

Legal Issues: I am not a lawyer

- Our Supreme Court Judges dress like Santa…

CloudPassage

Legal Issues: I am not a lawyer

- You don't want legal advice from me (us)…

CloudPassage

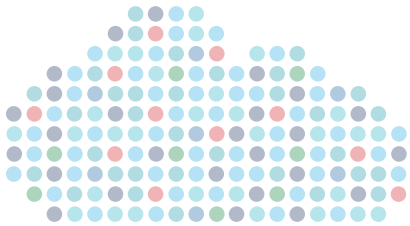
Legal Issues

- Expectation of privacy
- Possession, custody, control
- Data preservation
- Jurisdiction
- Seizing Data

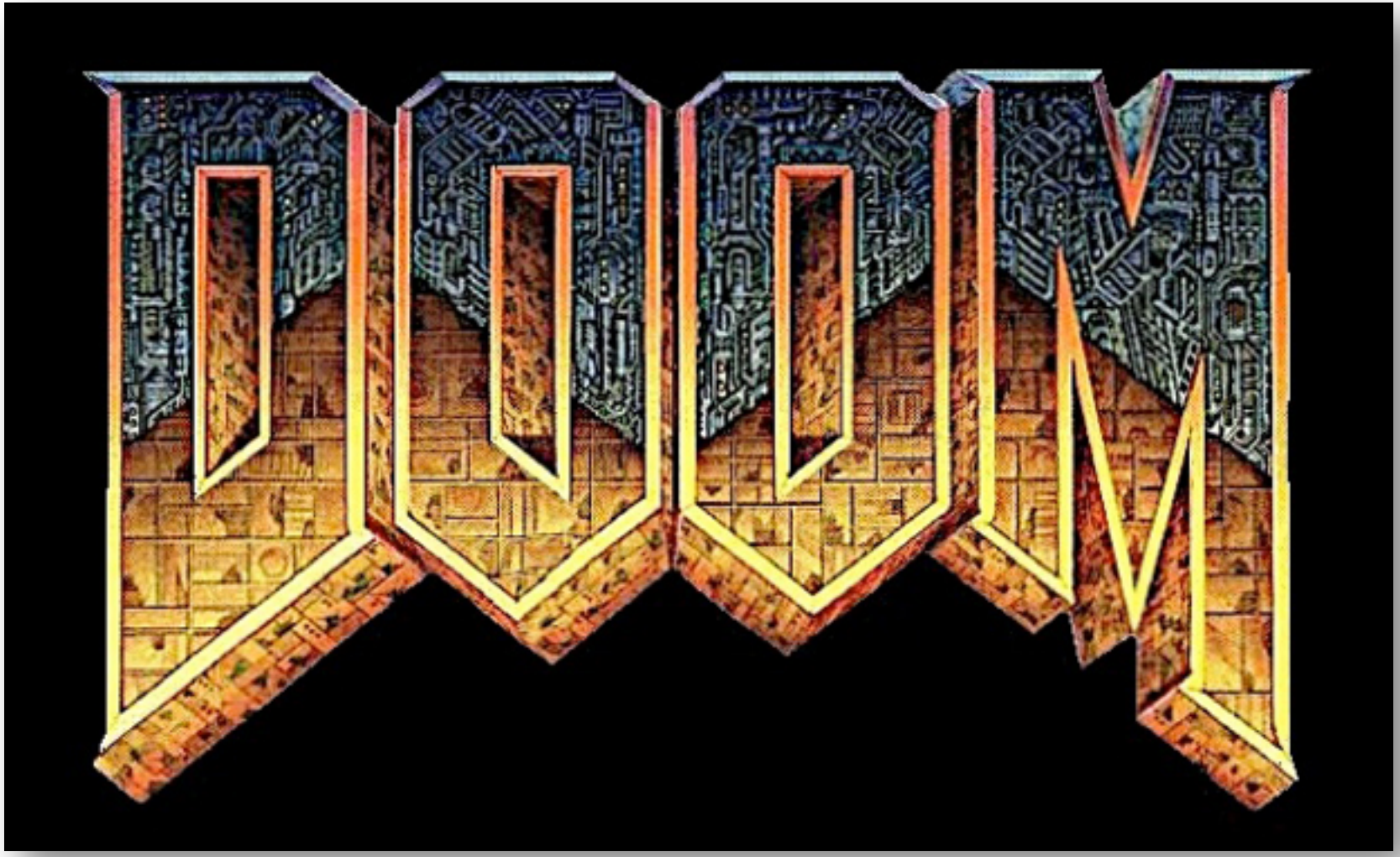
CloudPassage

How Existing Forensics/IR Tools Can Help

…And What They Can Do Better



It's Not All…



CloudPassage

And It's Not All Gloom…

CloudPassage

Great Quote…

"*Cloud forensic tools need to be a **hybrid** of the current **static** and **live collection and analysis** methods, and they need intelligence to note and predict artifacts based on forensic heuristics.*" – Zimmerman and Glavach, IAnewsletter Vol 14 No 1 Winter 2001

CloudPassage

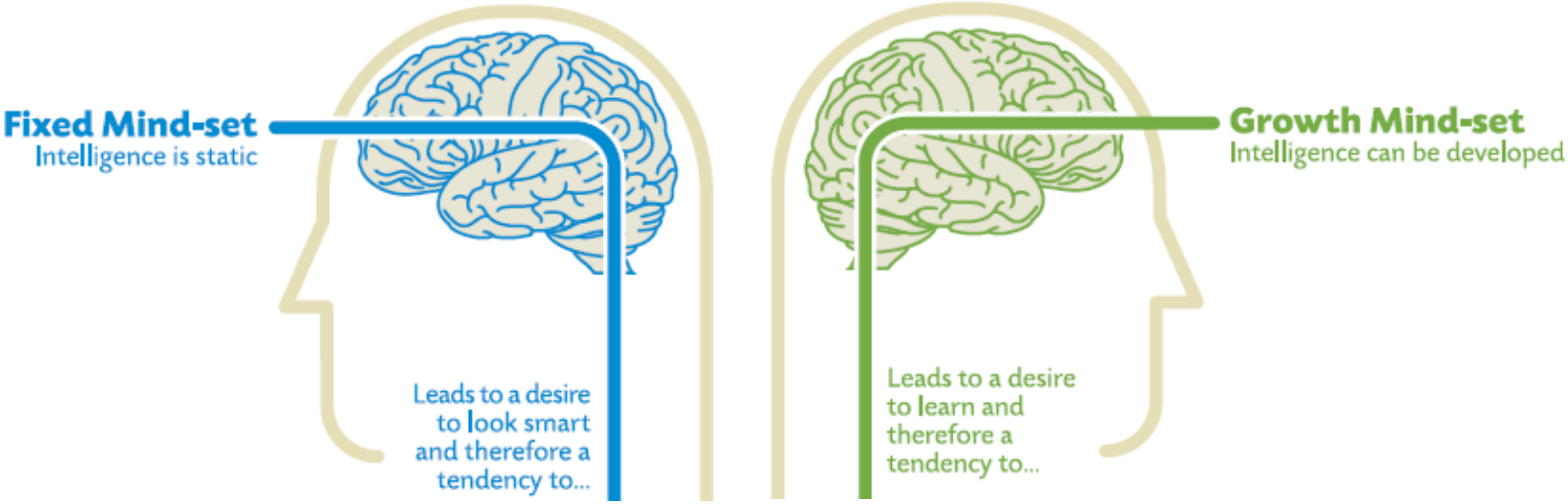
New Architecture, Similar Tools

- Your old tools and techniques may still work
  - Some, but not all

CloudPassage

Not Just Technical Challenges

- **Biggest challenge is mindset**
- **Need to grow comfortable with**
  - Storing images/data/ off-site (*a.k.a. The Cloud*)
  - Processing off-site (*a.k.a. The Cloud*)
  - Launching off-site analysis consoles in…you guessed it, *The Cloud*!

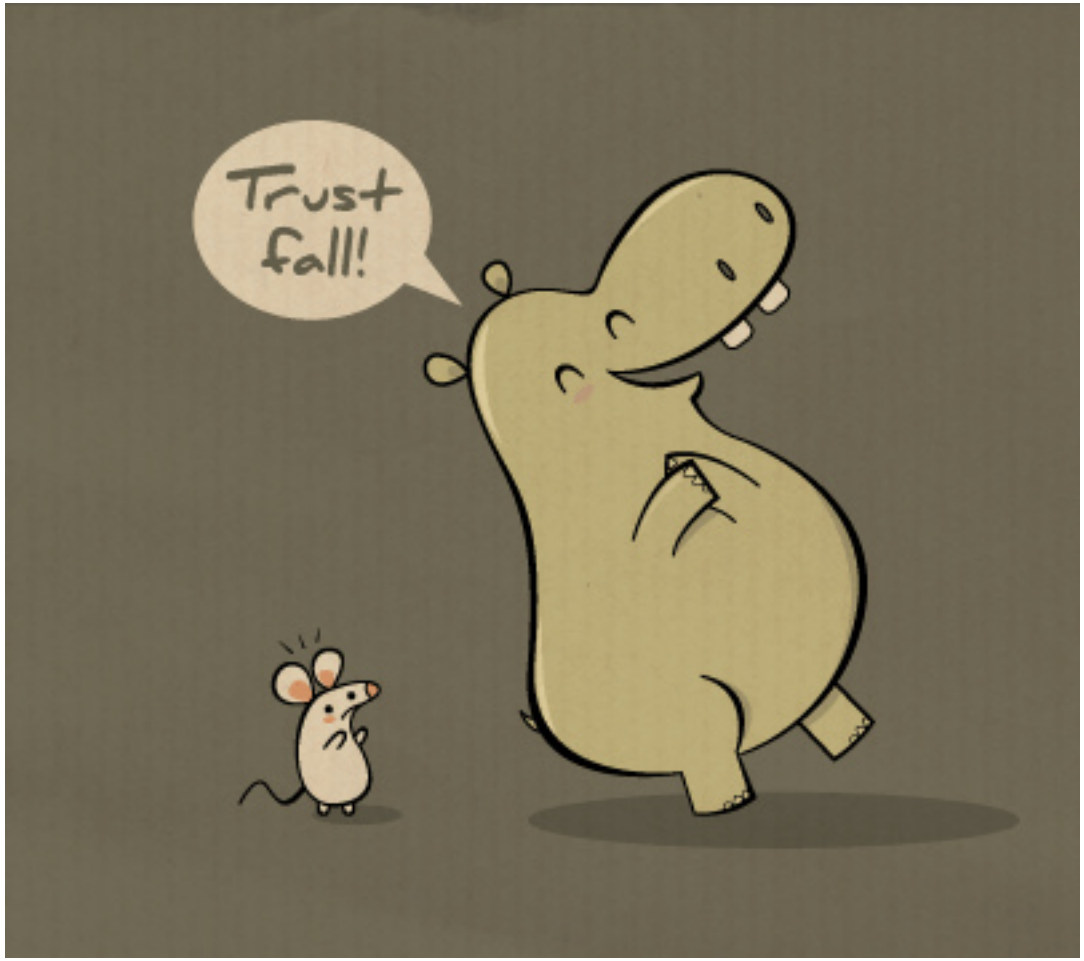


CloudPassage

It's Not This Easy…

CloudPassage

Or Even This Easy…

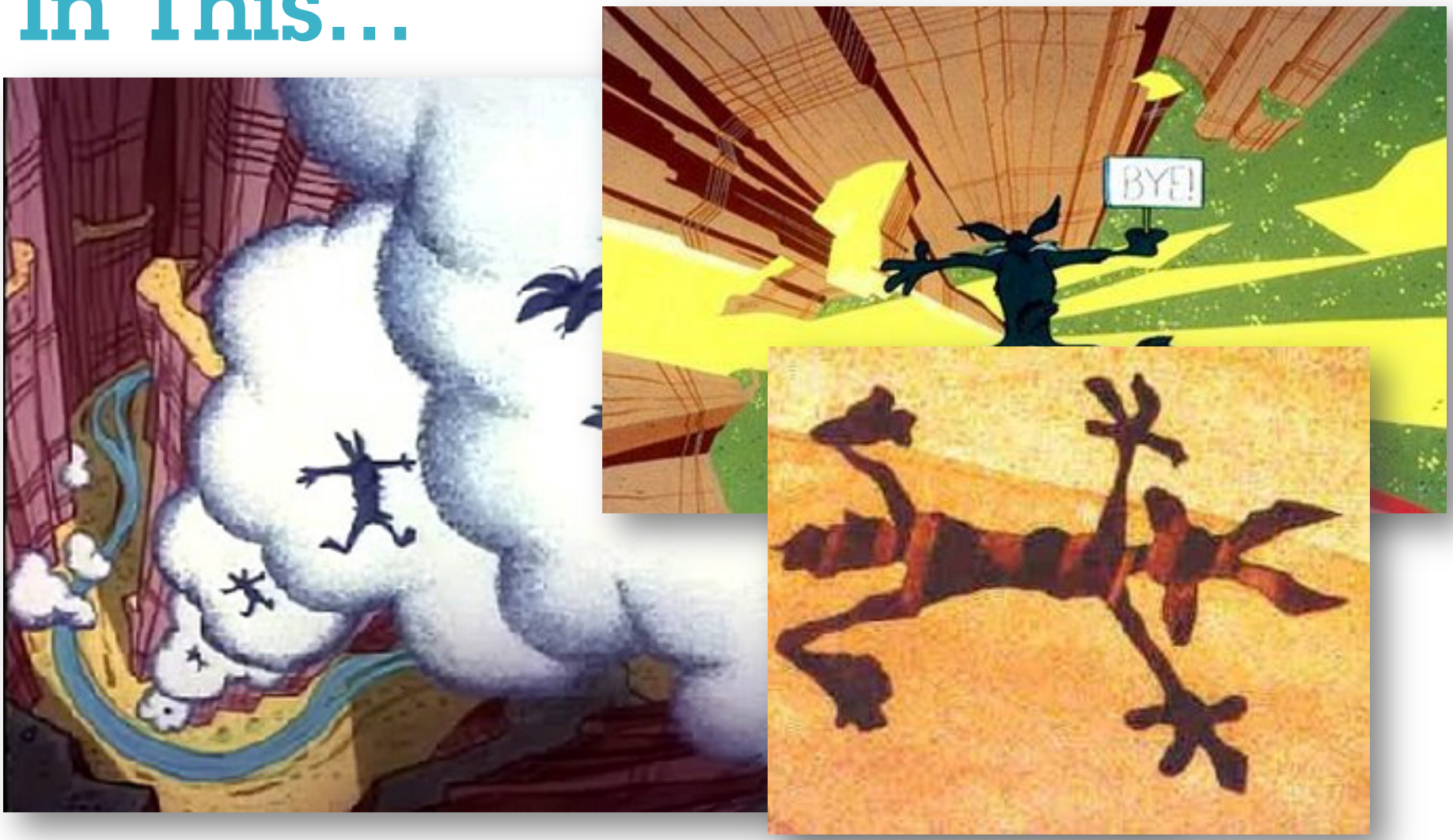


CloudPassage

It's More Like This…

CloudPassage

That Hopefully Doesn't Result In This…



CloudPassage

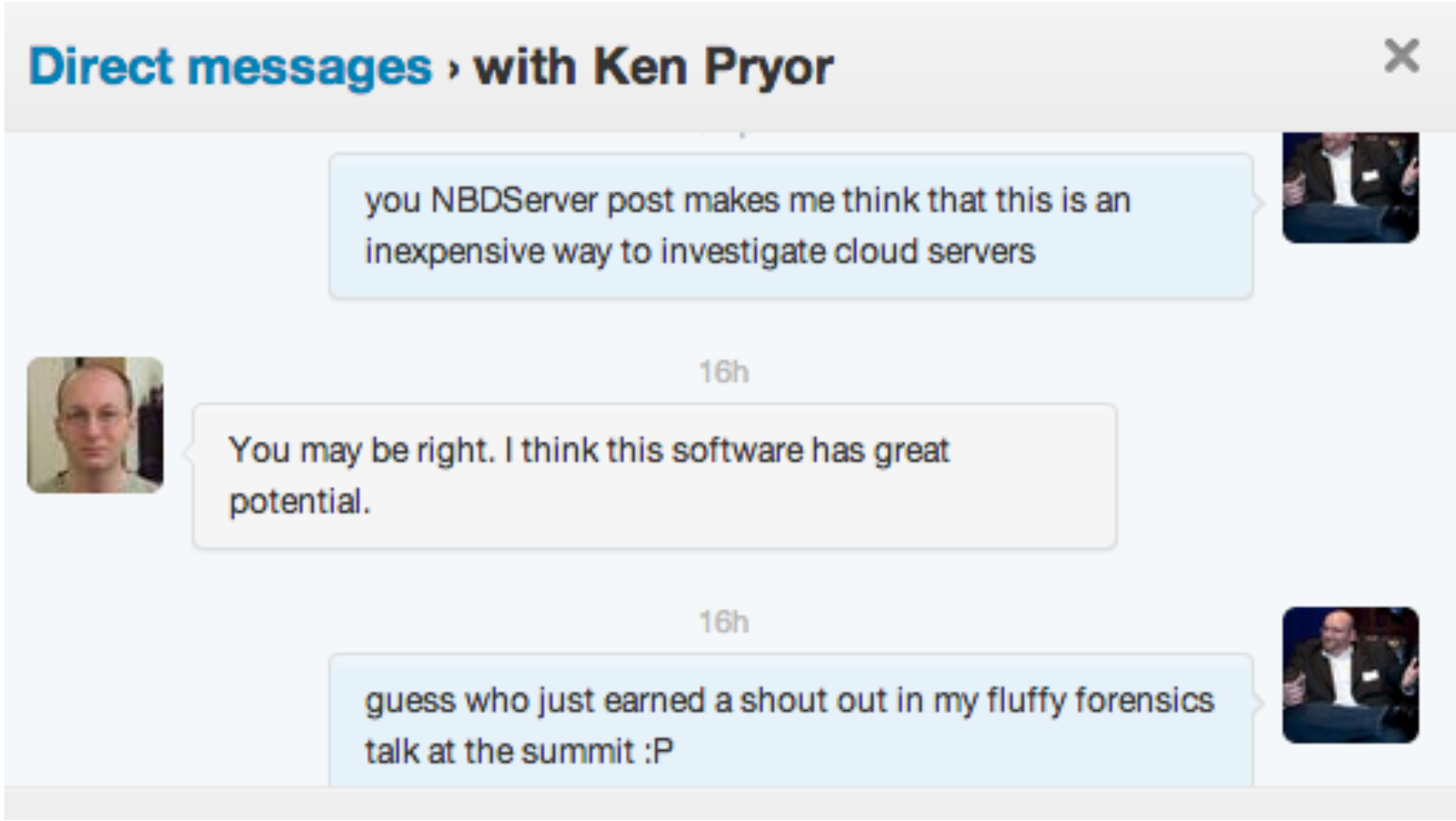
Existing Tools Can Be Used…

e.g. NBDServer

- Serves the (XP, Win 7, Win 2008) server as a read-only network block device
- Also possible to use this tool (w/Volatility) to image the Windows system RAM across the network to your client

https://github.com/jeffbryner/NBDServer

Special Thanks to @KDPryor



Post: http://digiforensics.blogspot.com/2013/04/nbdserver.html

CloudPassage

So I Was Going To Do a Demo…

…And That Didn't Work Out

CloudPassage

Of Course…I Had Some Problems

Andrew Hay @andrewsmhay 19h

checking for GLIB - version >= 2.26.0... no
*** Could not run GLIB test program, checking why...

wwwhhhhhyyyyyyyy!?!?!?!?!?!

Collapse Reply Delete Favorite ••• More

12:09 PM - 17 Apr 13 · Details

Reply to @andrewsmhay

ltawfall @ltawfall 18h

@andrewsmhay Ubuntu hates you.. and me for that matter but slightly less than old version of CentOs

Expand

CloudPassage

Existing Tools Can Be Used…

[server] `nbdserver.exe -c 192.168.2.197 -f \\.\PHYSICALDRIVE0 -n0`

[client] `modprobe nbd`

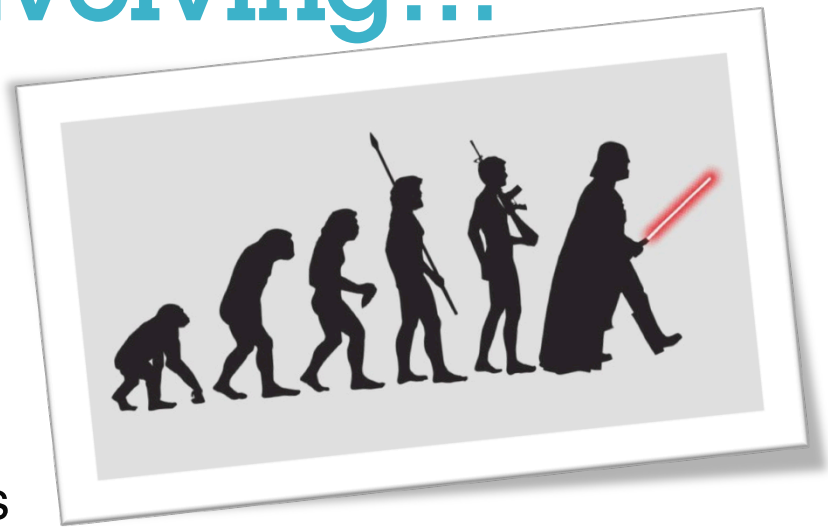
[client] `nbd-client 192.168.2.157 60000 /dev/nbd0`

 # This starts the client, tells it to look for the server on 192.168.2.157, use port 60000 and create the new network block device as /dev/nbd0.

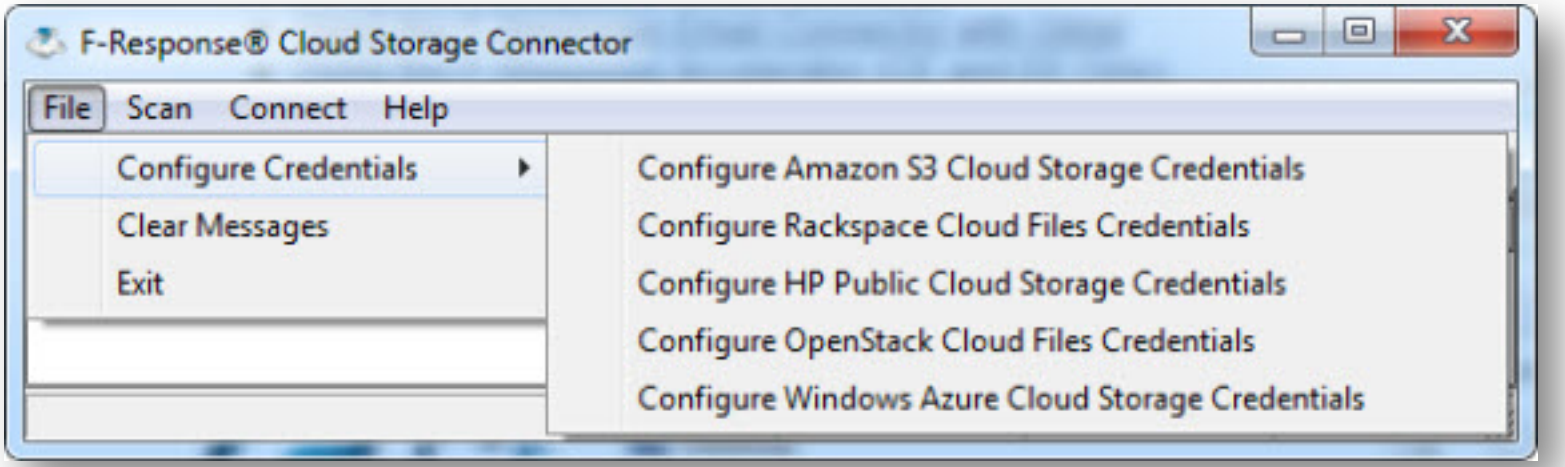
[client] `fls -f ntfs -m C: -r /dev/nbd0 > test.fls`

CloudPassage

Existing Tools Are Evolving…



- **F-Response 4.0.4**
  - And the new Cloud Connector
  - Let's you 'mount'
    - Amazon S3 Buckets
    - HP, Rackspace Cloud Containers
    - Windows Azure Blob Storage Containers



CloudPassage

Chad Tilbury's Blog Post

Like many great inventions, the idea behind F-Response is so simple and elegant it is hard not to punish yourself for not thinking of it. Using the iSCSI protocol to provide read-only mounting of remote devices opens up a wealth of options for those of us working in geographically dispersed environments. I have used it for everything from remote imaging to fast forensic triage to live memory analysis. F-Response is vendor-neutral and tool independent, essentially opening up a network pipe to remote devices and allowing the freedom of using nearly any tool in your kit. The product is so good, I really wouldn't blame them for just sitting back and counting their money. Luckily, counting money gets boring fast, so instead the folks at F-Response have kept innovating and adding value. Their latest additions are new "Connector" tools: Database, Cloud, and Email.

REF: http://forensicmethods.com/fresponse-cloud-forensics

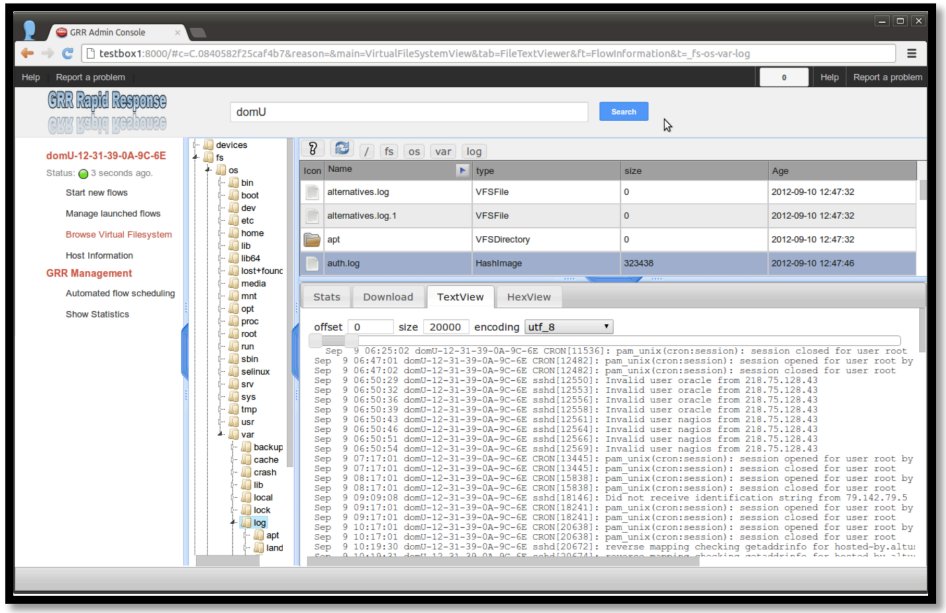
CloudPassage

New Tools Are Popping Up

- GRR
  - Incident Response Framework focused on Remote Live Forensics

Why GRR?

- Tell me if this machine is compromised
  - (while you're at it, check 20000 of them)
- Joe saw something weird, check his machine
  - (p.s. Joe is on holiday in Cambodia and on 3G)
- Why did a packet containing "fooooo" go from A to B?
  - (by the way, we're not sure what A was)
- Forensically acquire 25 machines for analysis
  - (p.s. they're in 5 continents and none are Windows)




```
# wget https://grr.googlecode.com/files/install_script_ubuntu_12.sh
# bash install_script_ubuntu_12.sh 2>&1 | tee grr_install.log
```

Source: Darren Bilby, Google – *GRR Rapid Response* – OSFC2012

CloudPassage

GRR Rapid Response Presentation

- https://code.google.com/p/grr/downloads/detail?name=GRR%20Rapid%20Response%20-%20OSFC%202012.pdf

File: GRR Rapid Response - OSFC 2012.pdf 2.1 MB

Description: This presentation was given at the Open Source Forensics Conference on the first official release of GRR. http://www.basistech.com/about-us/events/open-source-forensics-conference/

SHA1 Checksum: 0e8f2b438a9cd94a1893ea28454d4ec387643c80 What's this?

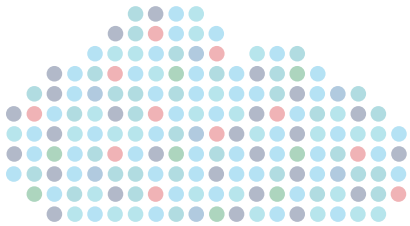
CloudPassage

Continued Evolution Required

- Cloud presents challenges
- Cloud also presents opportunities

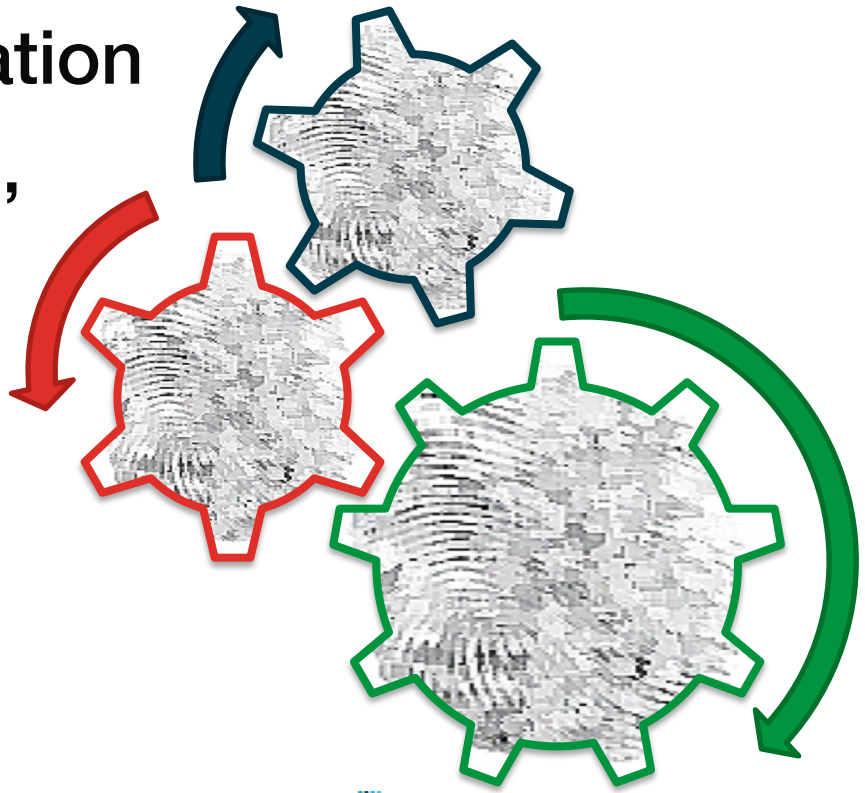
CloudPassage

Advantages Of Conducting Forensics/IR In Cloud Environments



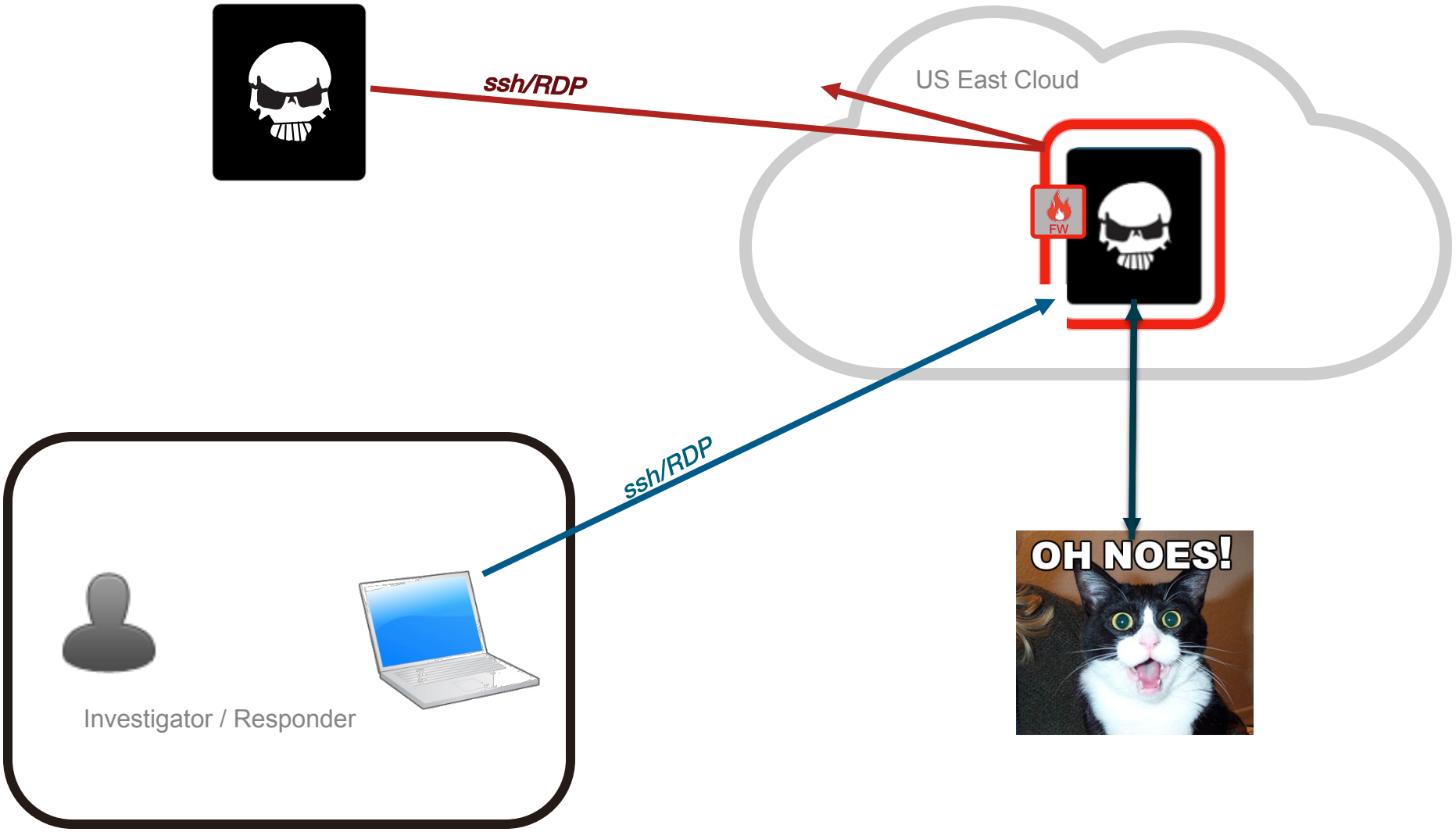
Advantages (now and future)

- Automated instance isolation
- On-demand forensic workbenches
- Automated timeline generation
- Dynamic analysis ‘workers’
- Distributed file carving
- Multi-cloud analysis



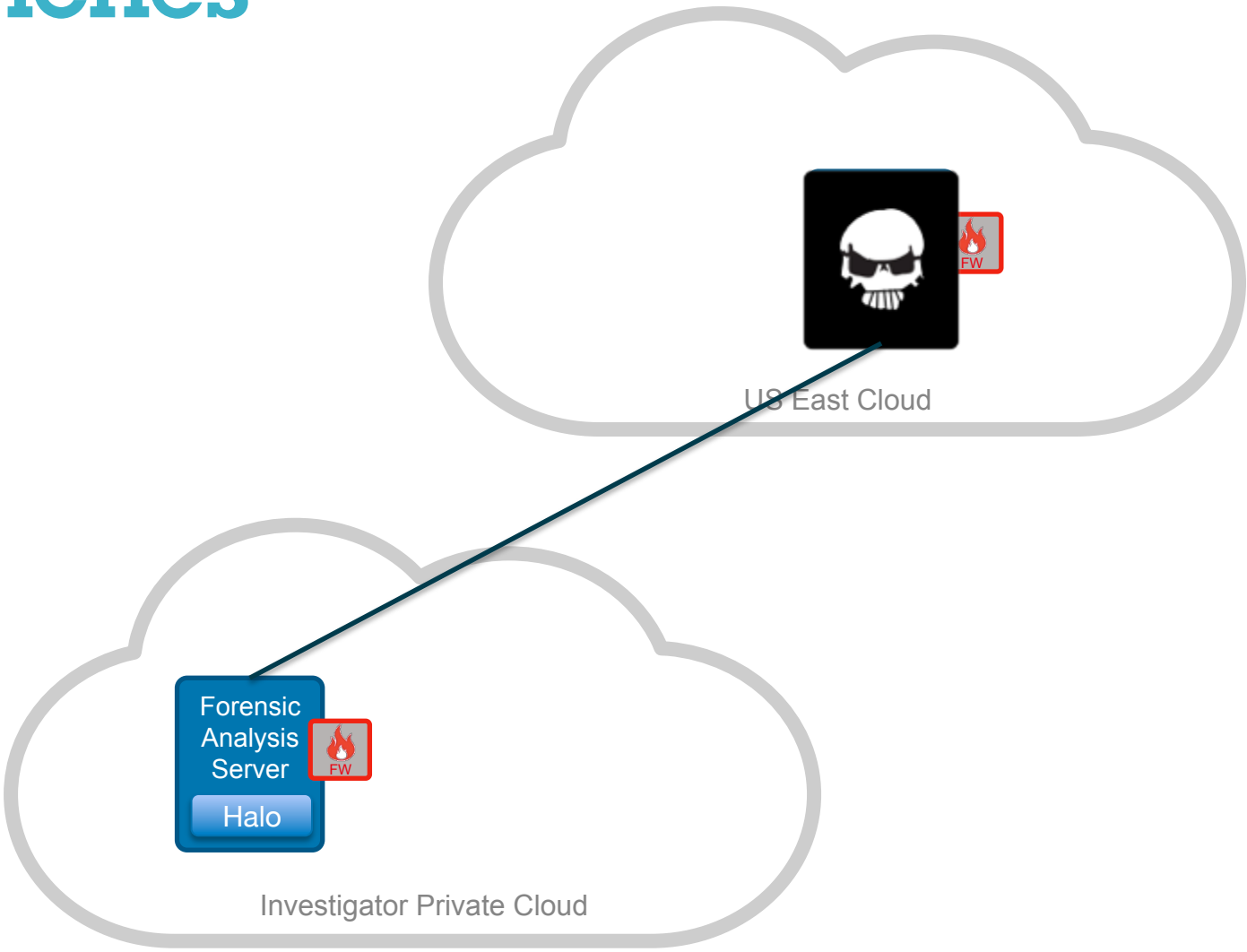
CloudPassage

Automated Instance Isolation



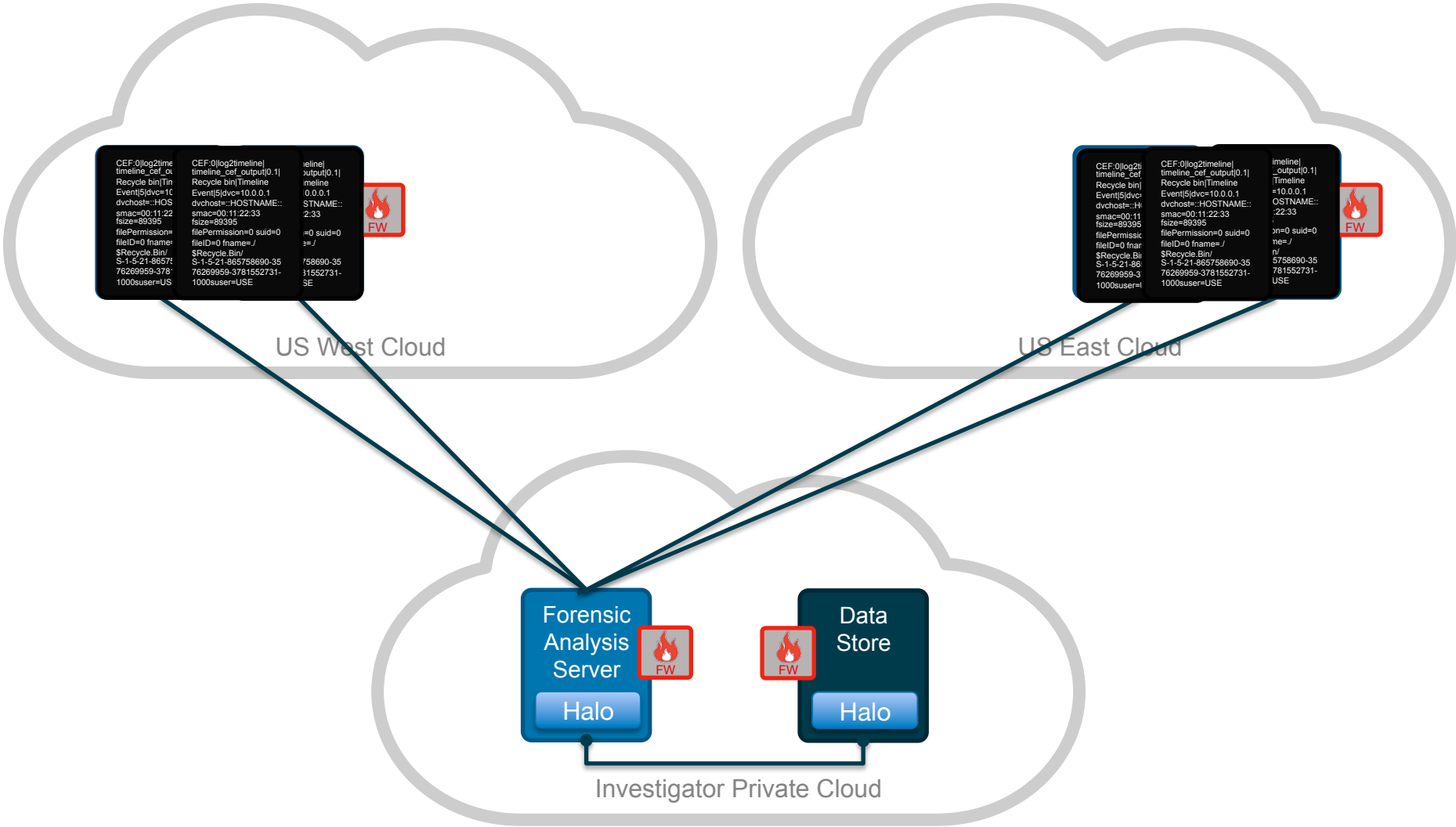
CloudPassage

On-demand Forensic Workbenches



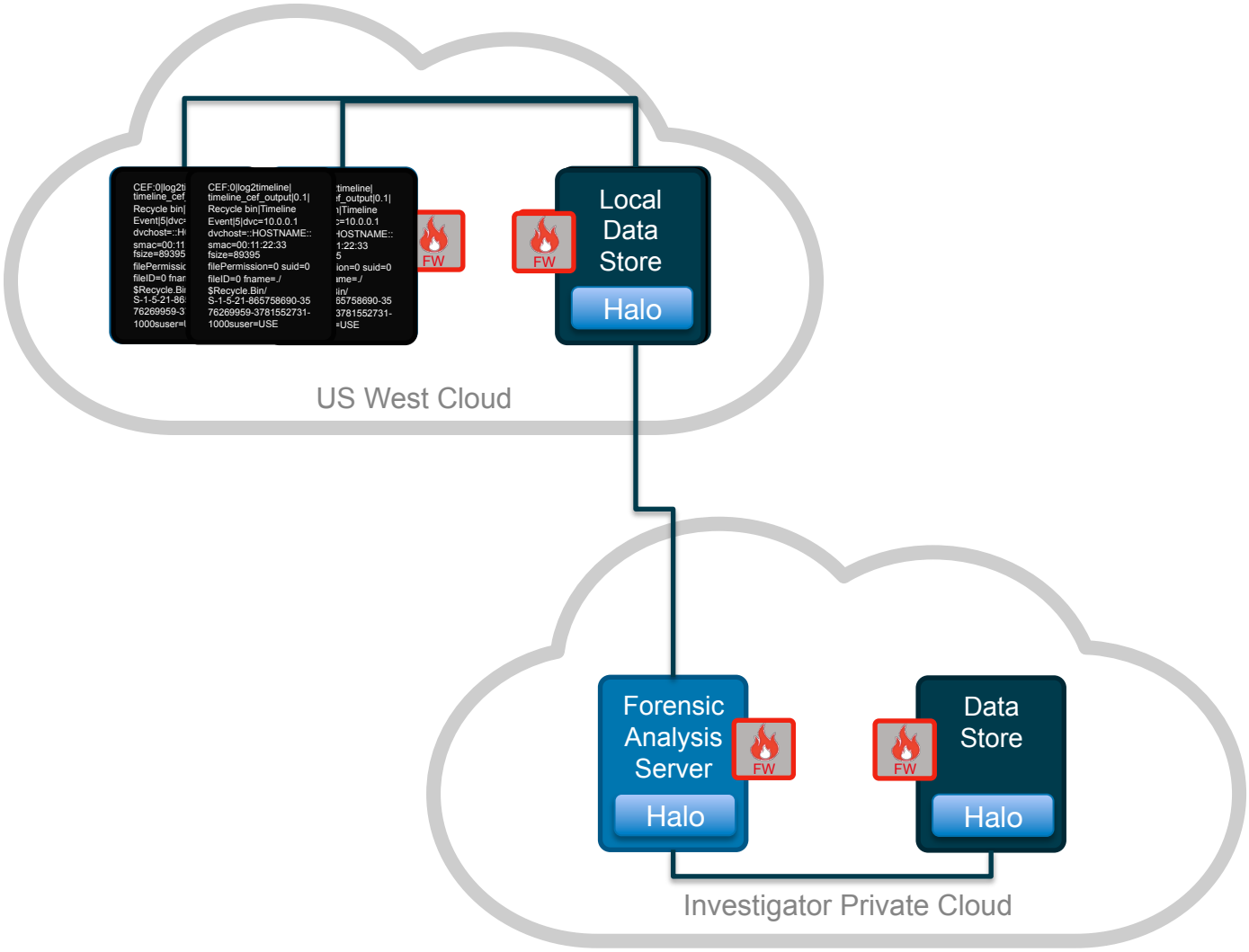
CloudPassage

Automated Timeline Generation



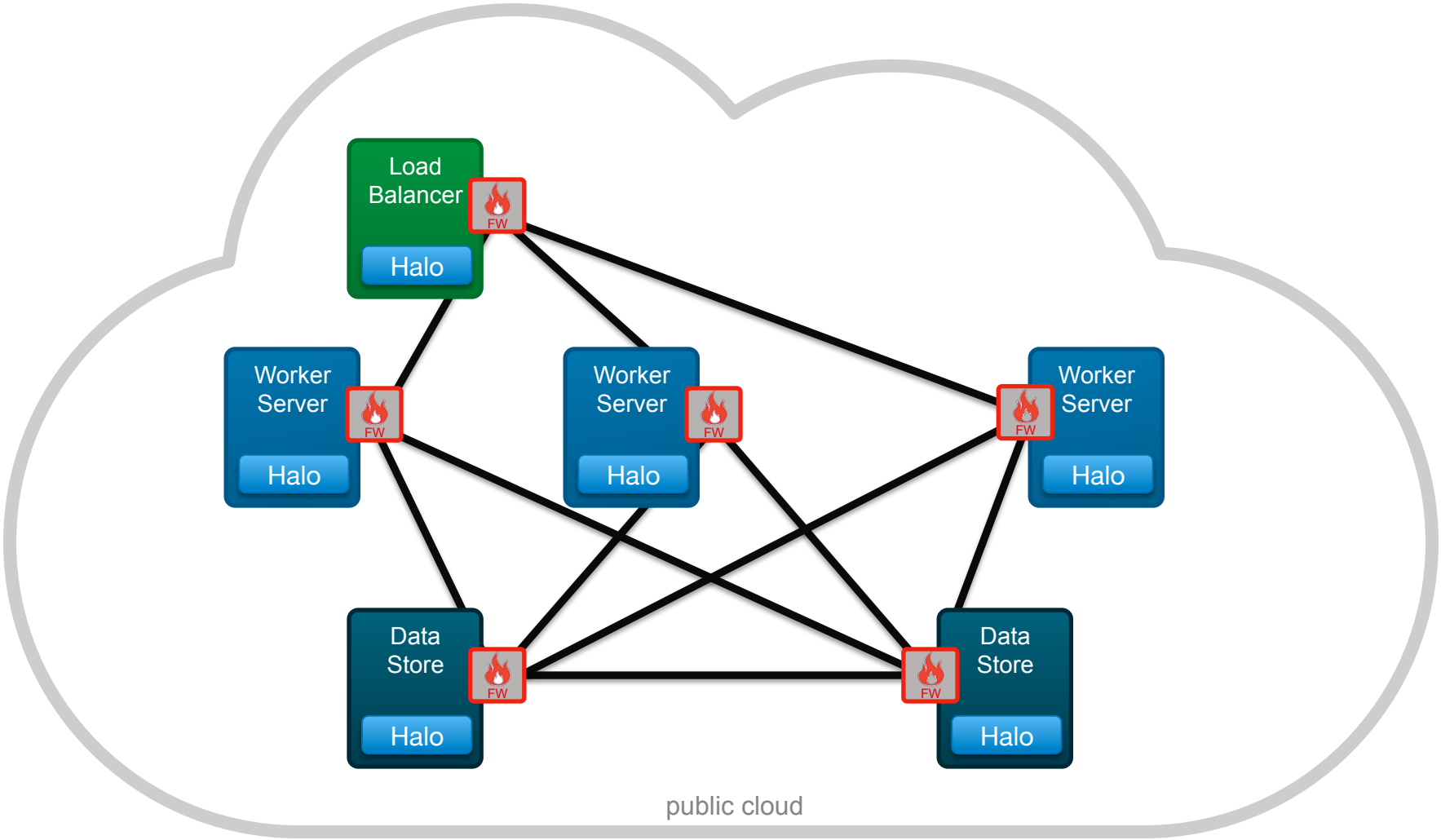
CloudPassage

Automated Timeline Generation



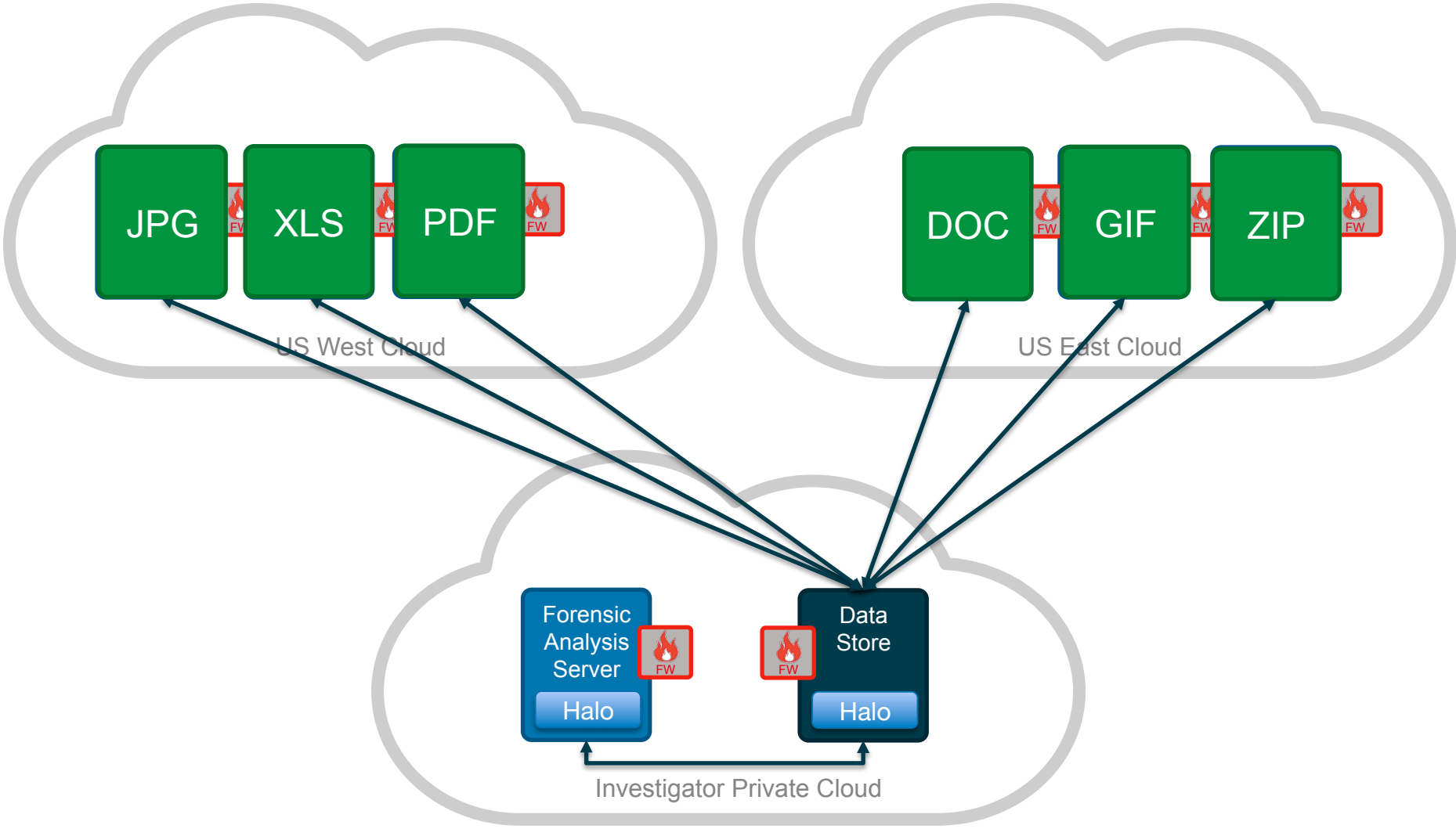
CloudPassage

Dynamic Analysis 'Workers'



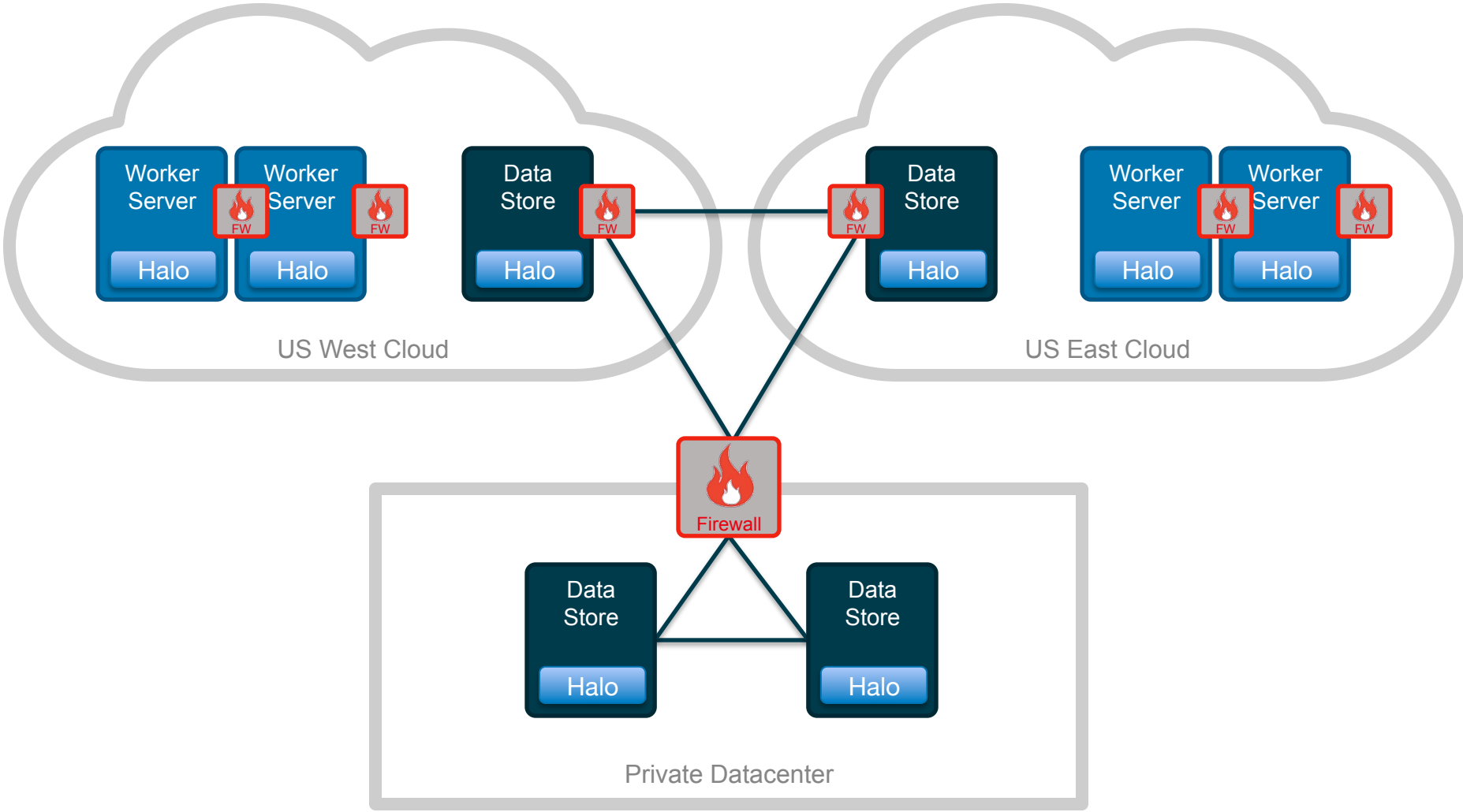
CloudPassage

Distributed File Carving



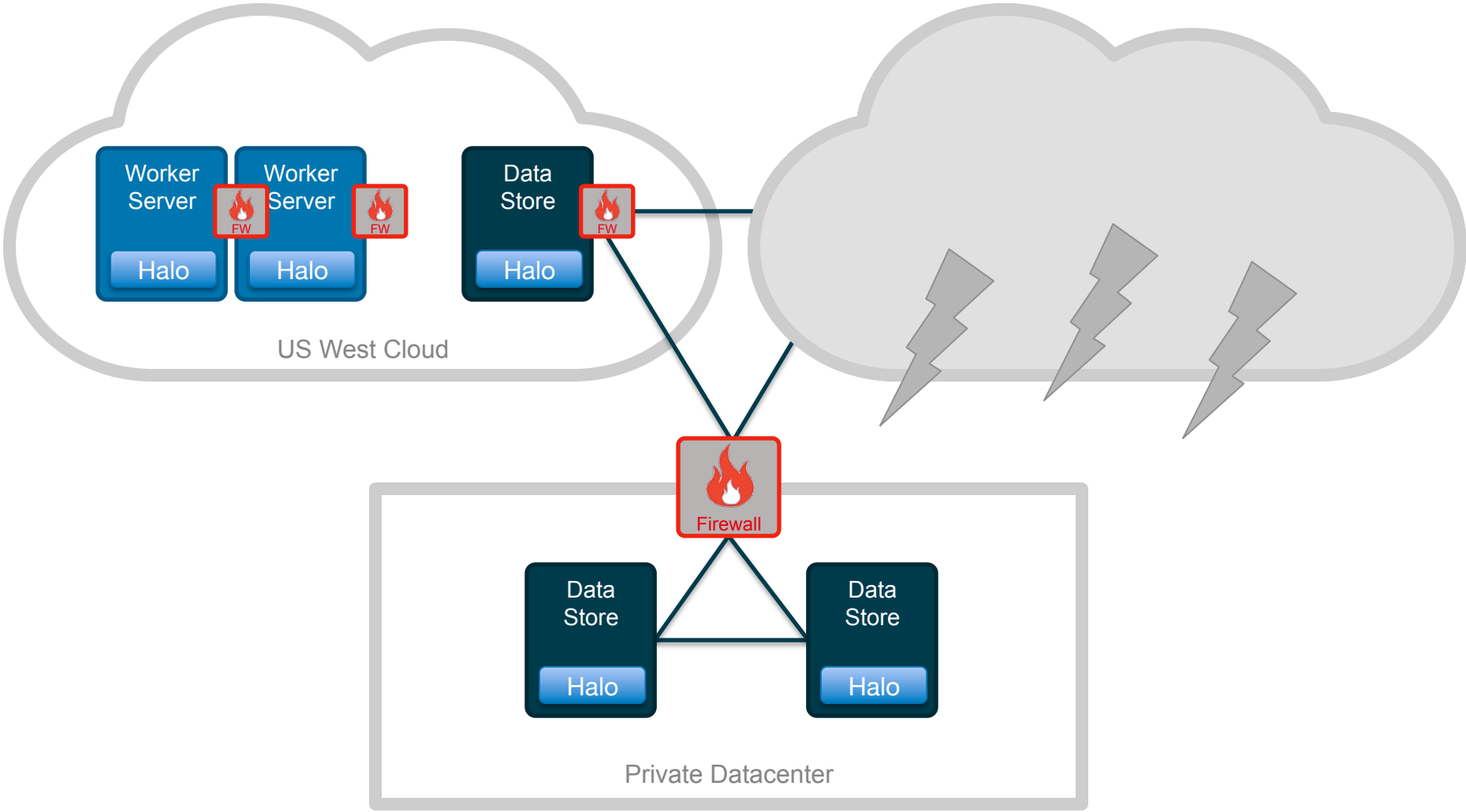
CloudPassage

Multi-Cloud Analysis Servers



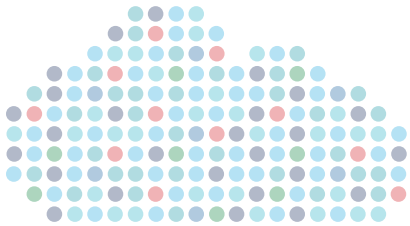
CloudPassage

Multi-Cloud Analysis Servers



CloudPassage

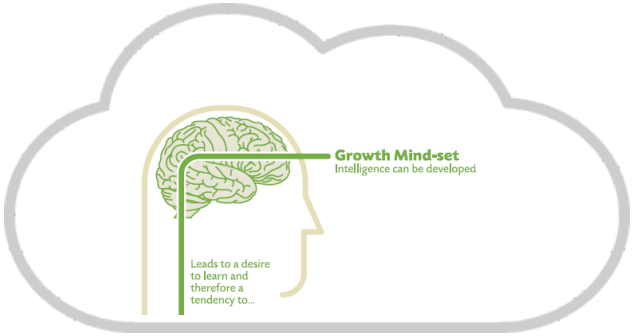
Summary



More Information

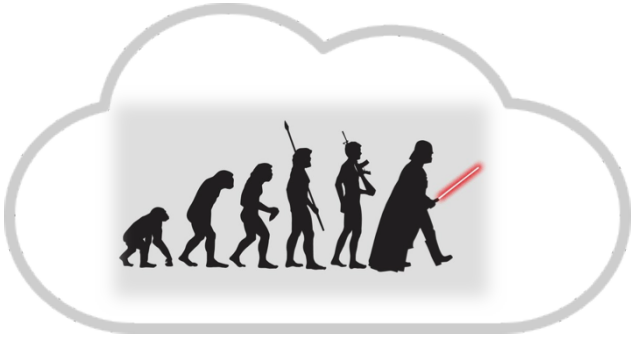
- NIST Special Publication 800-86 - Guide to Integrating Forensic Techniques into Incident Response
  - http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
- NIST Cloud Computing Forensic Science Working Group (NCC-FSWG)
  - http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudForensics
- Cloud Forensics Bibliography
  - http://www.forensicswiki.org/wiki/Cloud_Forensics_Bibliography

Summary



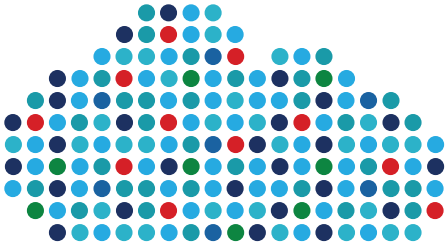
Cloud forensics and incident response require an open mind

Cloud can be used to help with complex investigations



Tools need to evolve to better handle dynamic environments

CloudPassage



Thank You

Andrew Hay

~~Chief Evangelist~~

Director of Applied Security Research

andrew@cloudpassage.com

twitter.com/andrewsmhay

CloudPassage