Sky-high IR

IR at Cloud Scale

@aarondlancaster

Who Am I?

@aarondlancaster

Aaron Lancaster

Sr. Security Engineer

Masters Student
@SANS_EDU

```
>>> dir(aaron_d_lancaster)
['__init__',
'__followChrist__',
'__loveWife__',
'__raiseKids__',
'__flyHelos__',
'__flyDrones__',
'assess_environments',
'call_CQ',
'defend_networks',
'handle_incidents',
'mentor_infosec',
'write_python']
```

WARNING: Several PEPs were broken in the making of this slide… sorry.

Agenda

1. Strategic, tactical, and legal implications
2. Supporting architecture & scenarios
3. Industry trends & tools
4. Critical components, crown jewels and compromise
5. Q&A

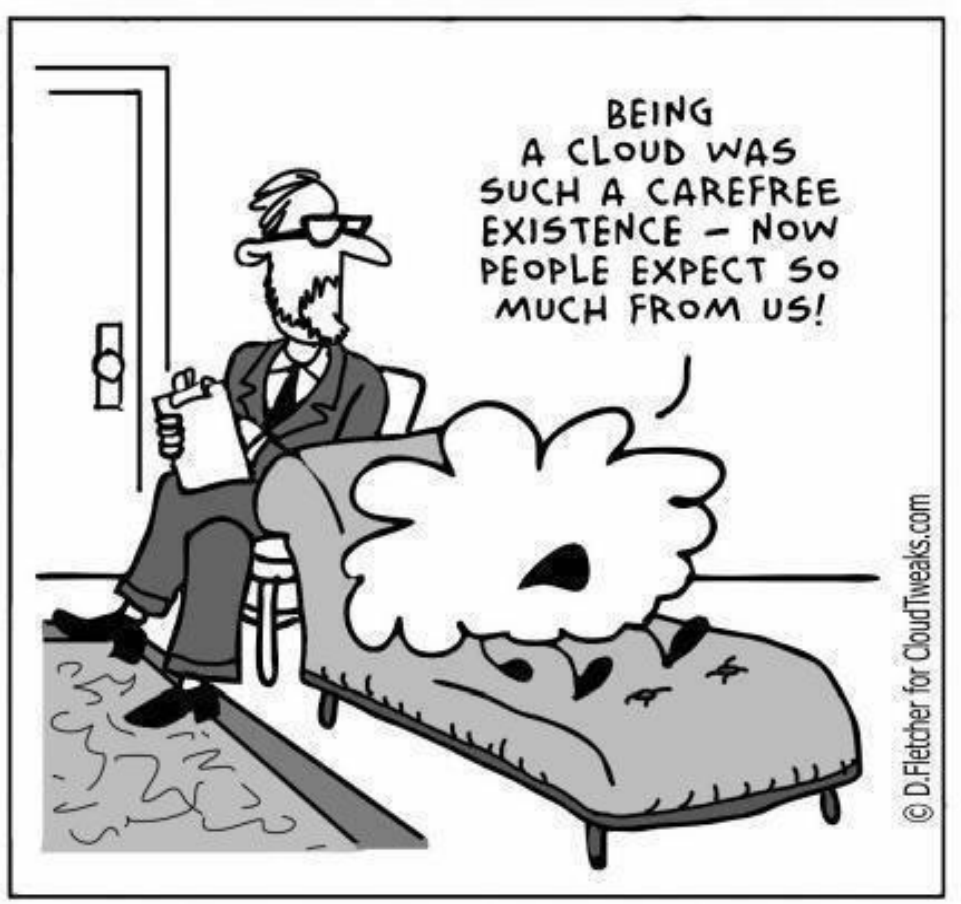
NO LEGAL ADVICE INTENDED

OPINIONS ARE MY OWN

DISCLAIMER:
The materials available herein and via linked websites are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem. The opinions expressed here or through linked sites are the opinions of the individual authors and may not reflect the opinions of their respective organizations, employers, or any individual attorney.

Link to slide and references will be provided at the end :-)

Rule #1: Know your audience


BEING A CLOUD WAS SUCH A CAREFREE EXISTENCE – NOW PEOPLE EXPECT SO MUCH FROM US!
© D.Fletcher for CloudTweaks.com


WHAT IF I TOLD YOU
"THE CLOUD" IS JUST
SOMEONE ELSE'S COMPUTER.

So there I was...

in a talk.

Inspiration

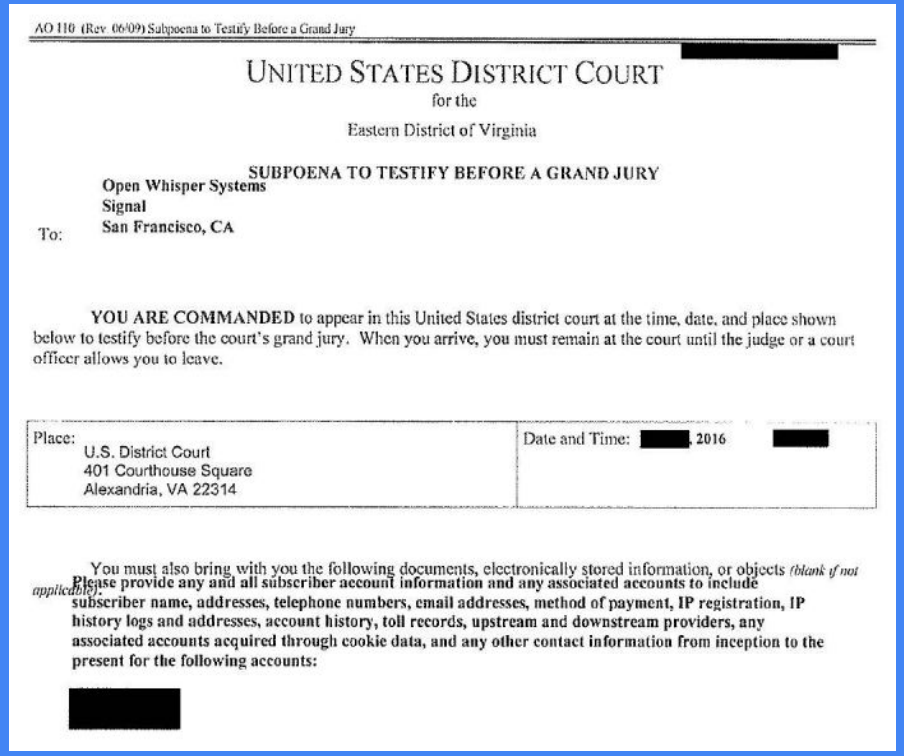
Legal Investigations

-Short notice

-Legal, ethical, self-preserving interest to comply

-Customer care

Subpoena



AO 110 (Rev. 06/09) Subpoena to Testify Before a Grand Jury [redacted]

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

SUBPOENA TO TESTIFY BEFORE A GRAND JURY

To: **Open Whisper Systems**
Signal
San Francisco, CA

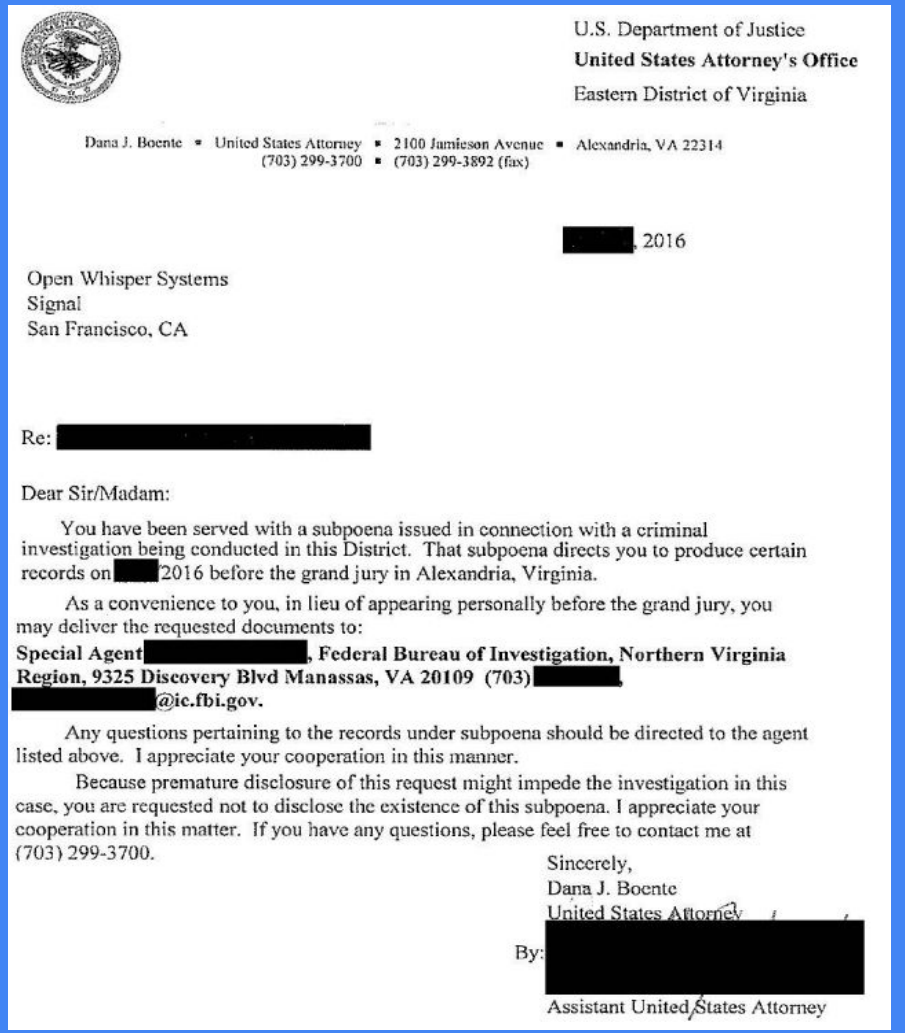
YOU ARE COMMANDED to appear in this United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place:	Date and Time:
U.S. District Court 401 Courthouse Square Alexandria, VA 22314	[redacted] 2016 [redacted]

You must also bring with you the following documents, electronically stored information, or objects *(blank if not applicable)*:

Please provide any and all subscriber account information and any associated accounts to include subscriber name, addresses, telephone numbers, email addresses, method of payment, IP registration, IP history logs and addresses, account history, toll records, upstream and downstream providers, any associated accounts acquired through cookie data, and any other contact information from inception to the present for the following accounts:

[redacted]



U.S. Department of Justice
United States Attorney's Office
Eastern District of Virginia

Dana J. Boente ▪ United States Attorney ▪ 2100 Jamieson Avenue ▪ Alexandria, VA 22314
(703) 299-3700 ▪ (703) 299-3892 (fax)

[redacted], 2016

Open Whisper Systems
Signal
San Francisco, CA

Re: [redacted]

Dear Sir/Madam:

You have been served with a subpoena issued in connection with a criminal investigation being conducted in this District. That subpoena directs you to produce certain records on [redacted] 2016 before the grand jury in Alexandria, Virginia.

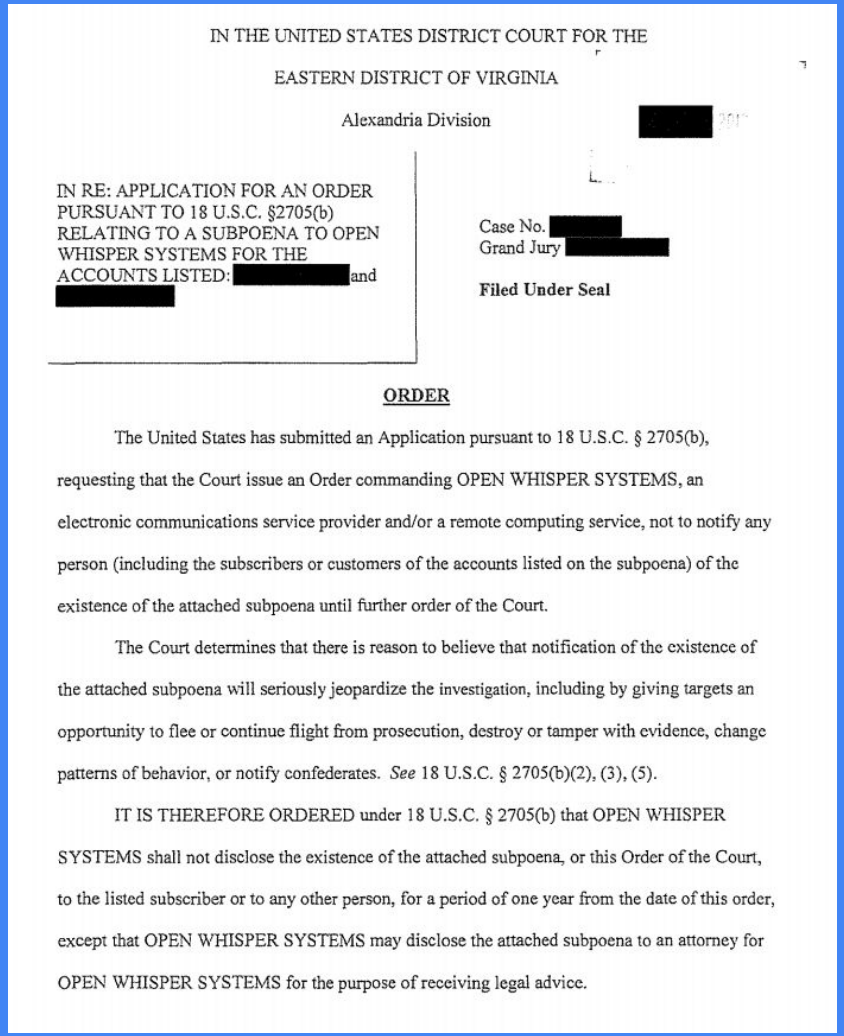
As a convenience to you, in lieu of appearing personally before the grand jury, you may deliver the requested documents to:
Special Agent [redacted], Federal Bureau of Investigation, Northern Virginia Region, 9325 Discovery Blvd Manassas, VA 20109 (703) [redacted] [redacted]@ic.fbi.gov.

Any questions pertaining to the records under subpoena should be directed to the agent listed above. I appreciate your cooperation in this manner.

Because premature disclosure of this request might impede the investigation in this case, you are requested not to disclose the existence of this subpoena. I appreciate your cooperation in this matter. If you have any questions, please feel free to contact me at (703) 299-3700.

Sincerely,
Dana J. Boente
United States Attorney

By: [redacted]
Assistant United States Attorney



IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division [redacted]

IN RE: APPLICATION FOR AN ORDER PURSUANT TO 18 U.S.C. §2705(b) RELATING TO A SUBPOENA TO OPEN WHISPER SYSTEMS FOR THE ACCOUNTS LISTED: [redacted] and [redacted]

Case No. [redacted]
Grand Jury [redacted]

Filed Under Seal

ORDER

The United States has submitted an Application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding OPEN WHISPER SYSTEMS, an electronic communications service provider and/or a remote computing service, not to notify any person (including the subscribers or customers of the accounts listed on the subpoena) of the existence of the attached subpoena until further order of the Court.

The Court determines that there is reason to believe that notification of the existence of the attached subpoena will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that OPEN WHISPER SYSTEMS shall not disclose the existence of the attached subpoena, or this Order of the Court, to the listed subscriber or to any other person, for a period of one year from the date of this order, except that OPEN WHISPER SYSTEMS may disclose the attached subpoena to an attorney for OPEN WHISPER SYSTEMS for the purpose of receiving legal advice.

Gag Order

Non disclosure
May not be time limited
NSLs

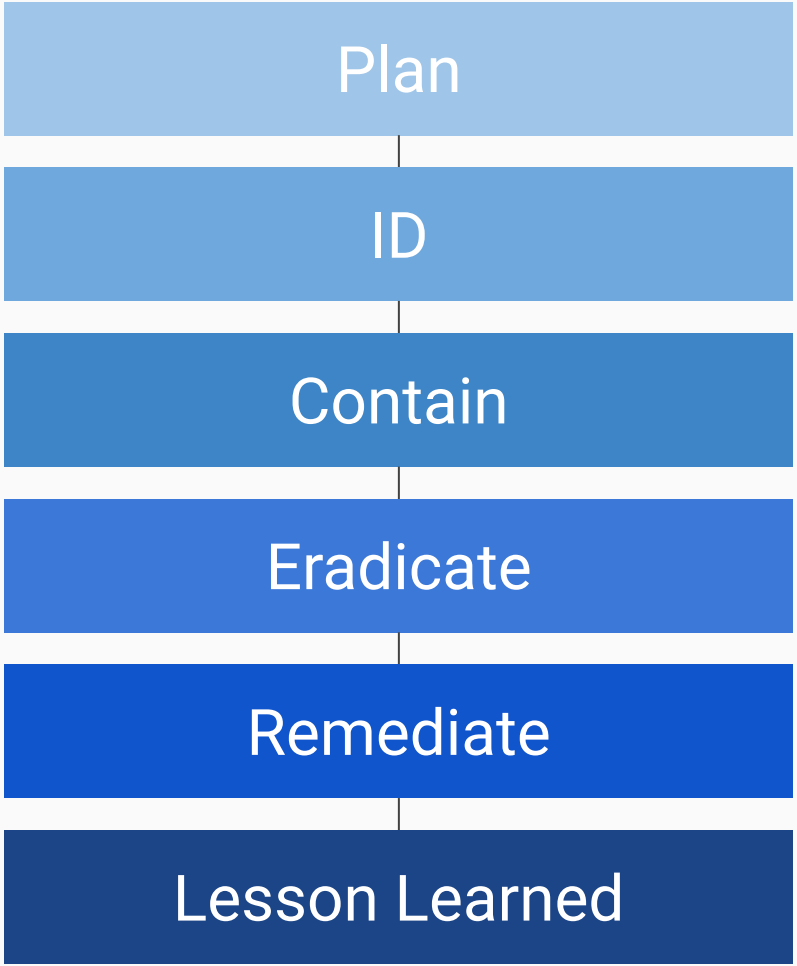
Microsoft v. DoJ

- Received over 3k gag orders 2014- early 2016
- ⅔ with no end date
- Argued Section 2705 of Stored Communications Act violates First Amendment
- 2017 - DOJ changed policy
  - Must demonstrate appropriate factual basis
  - Limited to one year
  - Barring exceptional circumstances

IR Process

Standardized Process for IR

Incident Handler's Handbook
by Patrick Kral - February 21, 2012



Scoping the response


ONE DOES NOT SIMPLY
"DOWNLOAD" PUBLIC CLOUD VM'S
imgflip.com

Microsoft:
making money off everyone since 1975

Outbound data transfers

(i.e. data going out of Azure data centers; zones refer to source region):

OUTBOUND DATA TRANSFERS	ZONE 1*
First 5 GB /Month [1]	Free
5 GB - 10 TB [2] /Month	$0.087 per GB
Next 40 TB (10 - 50 TB) /Month	$0.083 per GB
Next 100 TB (50 - 150 TB) /Month	$0.07 per GB
Next 350 TB (150 - 500 TB) /Month	$0.05 per GB
Over 500 TB /Month	Contact us

* For Zone details, please refer to the FAQ below.
[1] For monetary credit, 6-, and 12-month offers, outbound data transfer will be charged at the 5 GB - 10 TB tier.
[2] 1 TB = 1,024 GB

14TB = ~$1,200

Ref: https://azure.microsoft.com/en-us/pricing/details/bandwidth/

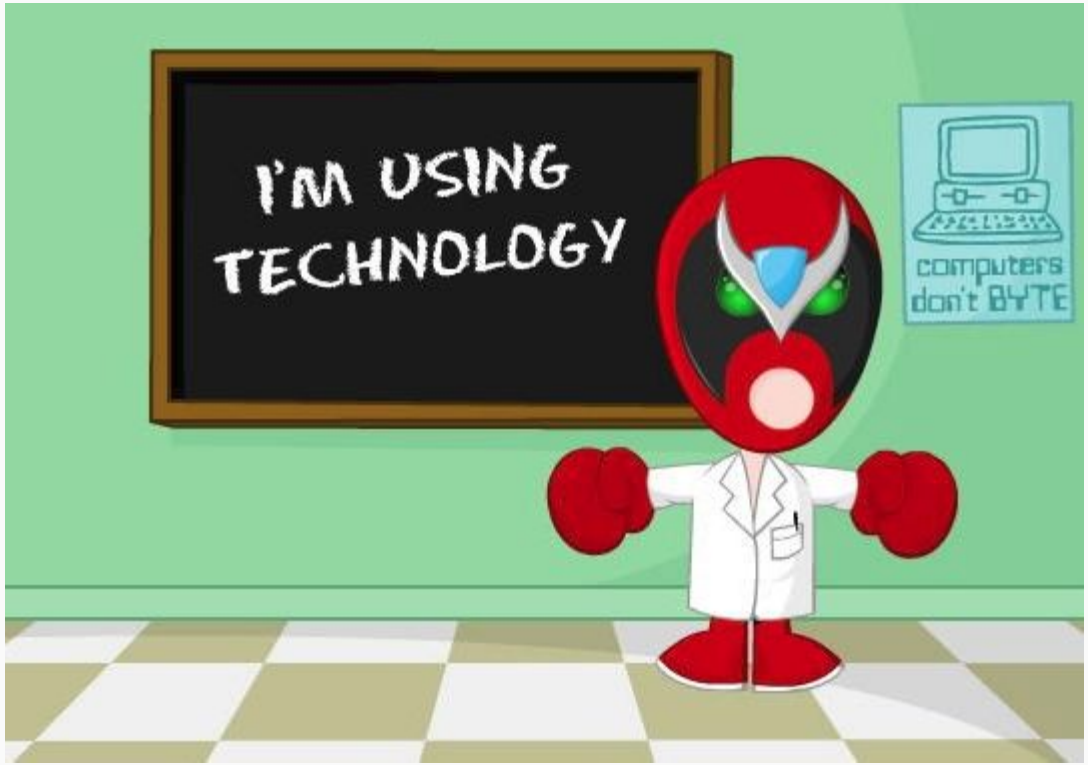
Amazon:
making money off “other” vendors since 2006

Data Transfer:

Inter-Region Data Transfer Out:	14000	GB/Week
Data Transfer Out:	0	GB/Month
Data Transfer In:	0	GB/Month
VPC Peering Data Transfer:	0	GB/Month
Intra-Region Data Transfer:	0	GB/Month
Public IP/Elastic IP Data Transfer:	0	GB/Week

Estimate of your Monthly Bill ($ 1324.40)

Ref: https://aws.amazon.com/blogs/aws/estimate-your-c/


I'M USING
TECHNOLOGY
computers
don't BYTE

Slicing Data

- ID exactly what is needed
- Surgically remove that
- Use compression if possible

Slicing with Python

- Use a module that understands existing structures (if there is one)
  OR
- Determine data format
- Determine delimiters based on format
- Load data in slices (supports large blobs)
- Save relevant slices
- Analyze with additional tools

S3QL - Creates a POSIX-like filesystem in user space (FUSE) using object storage or other storage as the target.

Major features:

- Encryption - 256-bit AES; also SHA-256 HMAC checksum
- Compression - pre-storage/pre-encrypt (LZMA, bzip2, or gzip)
- De-duplication - when files have identical content in part or full
- Copy-on-Write/Snapshotting - duplicate directory trees without the use of any additional storage space (target storage) - “incremental backup”
- Dynamic Size - can grow or shrink dynamically

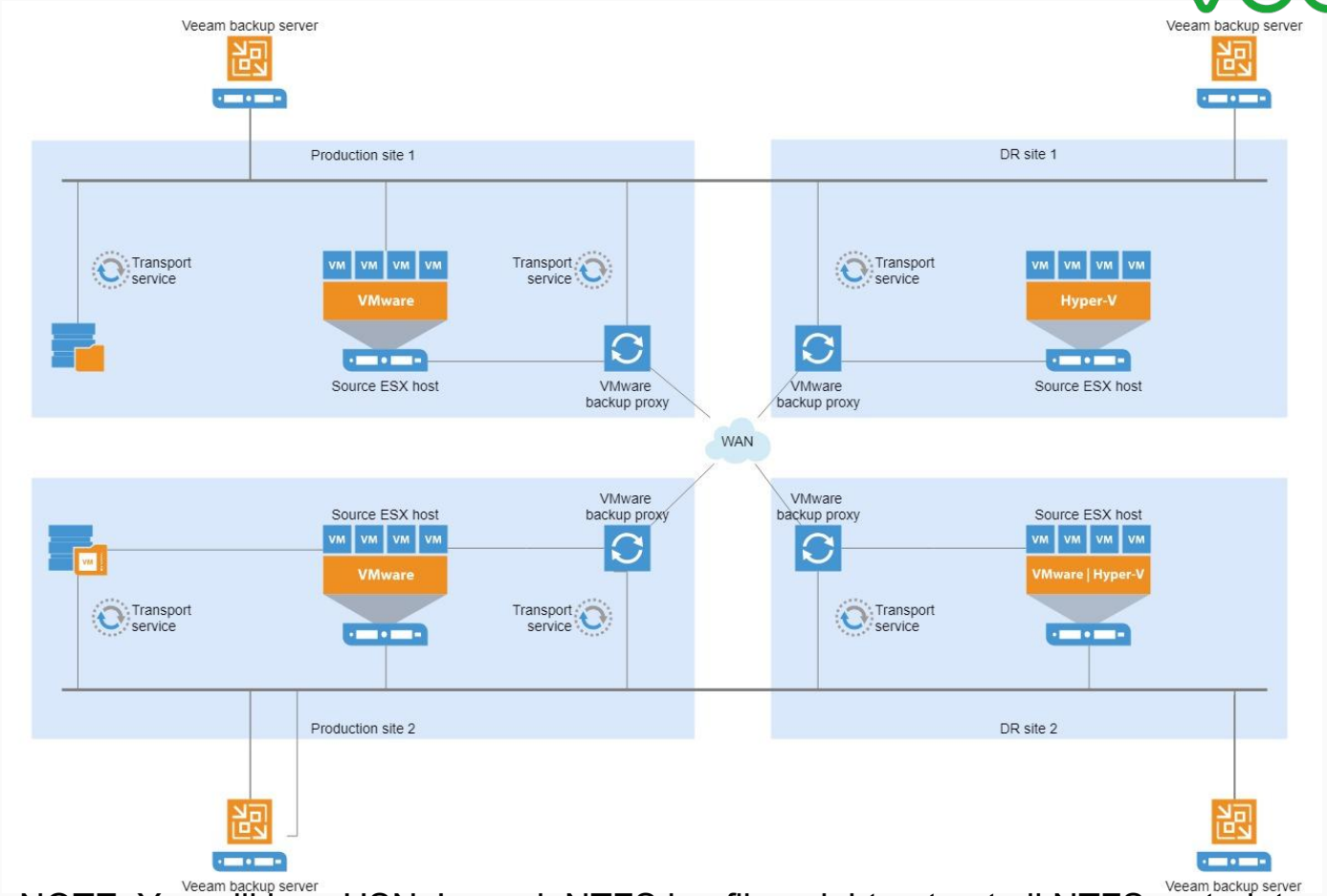
- Transparency - behaves like a local filesystem (supports hard links, symlinks, typical permissions, extended attributes (xattr) and file sizes up to 2TB)
- Immutable Trees - directory trees can be made immutable so that their contents can't be changed in any way whatsoever
- Range of Back-ends - supports Google storage, Amazon S3, Amazon Reduced Redundancy Storage (RRS), OpenStack Swift, Rackspace Cloud Files, S3-compatible targets, local filesystems, and even filesystems accessed using sshfs which are treated as a local filesystems.
- Caching - improve apparent performance, leverage local SSD for data caching

Scenarios & Supporting Architecture

- Move a large amount of data
- Ensure reliability
- Verify integrity

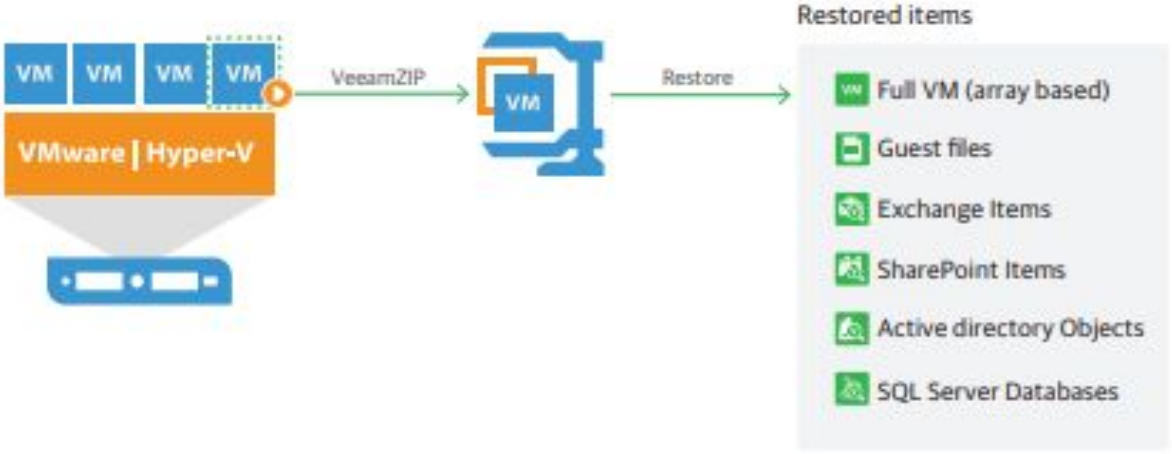
- Sounds like… ?

Backup Software - for more than just backups



NOTE: You will lose USN Journal, NTFS log file, might not get all NTFS metadata

Veeam Backup Free



VeeamZIP fully encapsulates the VM and makes ad hoc backups:

- **Easy:** No complicated configuration, and no need to power off the VM
- **Compact:** Compression and deduplication – as well as swap file, hibernation file and deleted files block exclusion and minimize backup size
- **Portable:** Captures all the virtual disks and configuration files needed to restore the VM on any host

- Native tape support
- End-to-end encryption
- Restore exactly what you need
- Instant File-Level Recovery
- Veeam Explorers (look into backups)
- Veeam Restore to Microsoft Azure
- File Manager...

Veeam FastSCP

-Alternative to using vSphere

-Requires management network connection

-Requires credentials

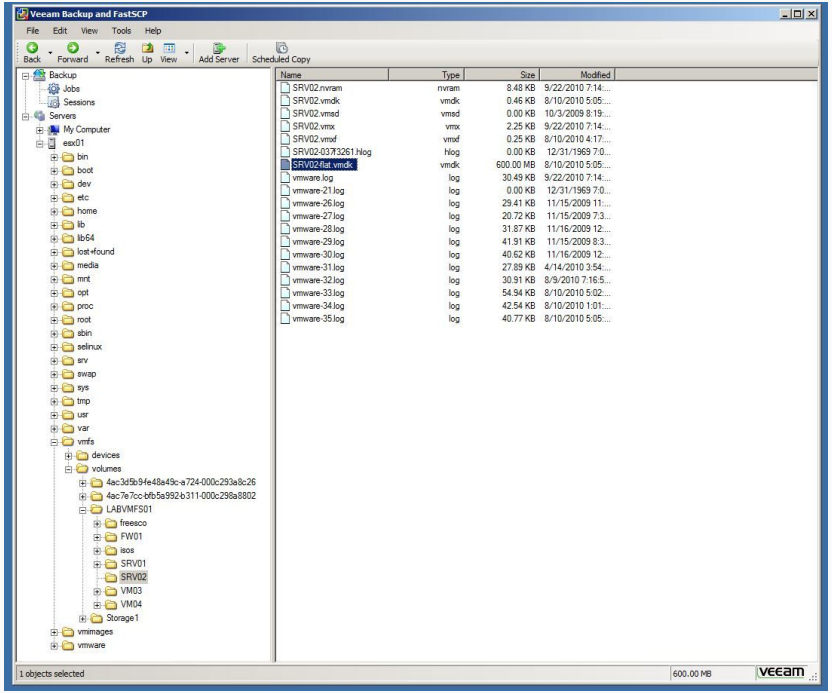
-Explorer-like interface - right-click copy

-Schedule a copy

-SSH Control Channel for session auth

-No ESXi unsupported mode change

-No additional services required



Credit: Paul Henry, SANS DFIR

Industry trends & tools

got sift?

Forensic workstation: SIFT

File system support

- NTFS (NTFS)
- iso9660 (ISO9660 CD)
- hfs (HFS+)
- raw (Raw Data)
- swap (Swap Space)
- memory (RAM Data)
- fat12 (FAT12)
- fat16 (FAT16)
- fat32 (FAT32)
- ext2 (EXT2)
- ext3 (EXT3)
- ext4 (EXT4)
- ufs1 (UFS1)
- ufs2 (UFS2)
- vmdk

Evidence Image Support

- raw (Single raw file (dd))
- aff (Advanced Forensic Format)
- afd (AFF Multiple File)
- afm (AFF with external metadata)
- afflib (All AFFLIB image formats (including beta ones))
- ewf (Expert Witness format (encase))
- split raw (Split raw files) via affuse
- affuse - mount 001 image/split images to view single raw file and metadata
- split ewf (Split E01 files) via mount_ewf.py
- mount_ewf.py - mount E01 image/split images to view single raw file and metadata
- ewfmount - mount E01 images/split images to view single raw file and metadata

Incident Response Support

- F-Response Tool Suite Compatible
- Rapid Scripting and Analysis
- Threat Intelligence and Indicator of Compromise Support
- Threat Hunting and Malware Analysis Capabilities

Software Includes:

- log2timeline (Timeline Generation Tool)
- Rekall Framework (Memory Analysis)
- Volatility Framework (Memory Analysis)
- bulk_extractor
- autopsy
- afflib
- dc3dd
- imagemounter
- libewf-python
- libvshadow
- log2timeline
- Plaso
- Qemu
- regripper and plugins
- SleuthKit
- 100s more tools

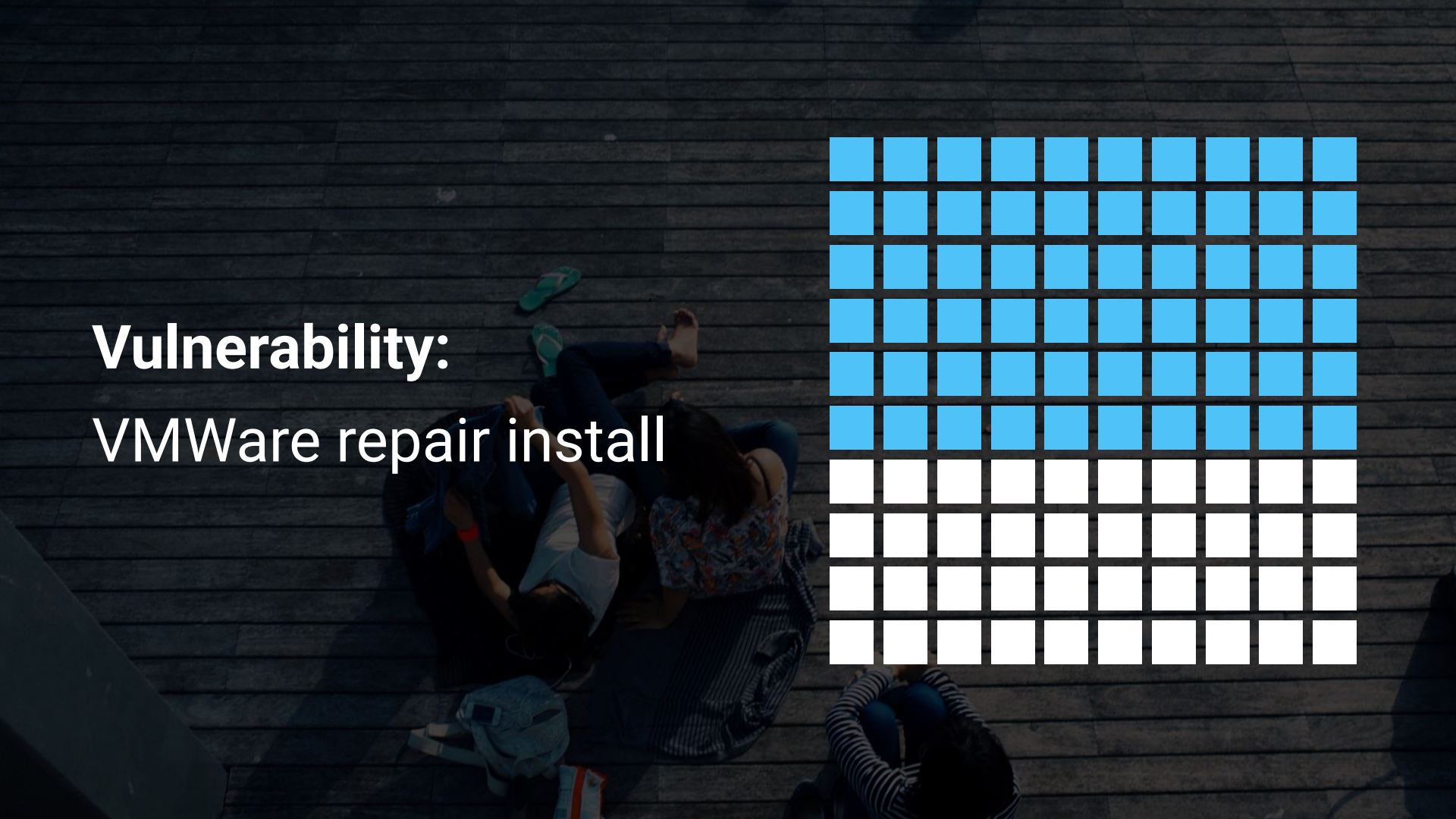
Ref: https://digital-forensics.sans.org/community/downloads#capabilities

Critical components, crown jewels & compromise

Attackers are after data where it’s:

- Stored
- Transmitted
- Processed

Use Case: Deleting Shadow Volume copies


Vulnerability:
VMWare repair install


FLAGRANT SYSTEM ERROR
The system is down. I dunno what
you did, moron, but you sure
screwed everythi
COMPY 386

Non-detection

Failure to log & alert

(or protect logs)

- Loss of logs => enable MFA delete on S3
- Account lockout => enable failed login event logging
- Data corruption => enable Object-level/Object Access logs
- Data loss => enable VPC flow / implement BRO, er… Zeek
- Un-noticed billing => enable CloudWatch billing alerts & events
- … and almost anything you can code in Python.

Overall:

- Implement a cloud-centric logging and threat management solution

Integrity

- Corrupt Stream by altering data
  - At origin (Persistence)
  - In flight (MiTM)
  - At destination (Phishing, DBDL)

Availability

- Disrupt job - DoS via
  - Vulnerability Scan
  - API
  - Critical Infra

All of these come back to monitoring, alerting and ability to respond.

Q&A

References

Thanks for listening!

What's your approach?

What did you think of mine?

https://goo.gl/zRtrXL

(https://blog.casterlan.com/2018/10/cloud-ir.html)