conference

Click ‘engage’ to rate session.

Rate **12** sessions to get the supercool GOTO reward

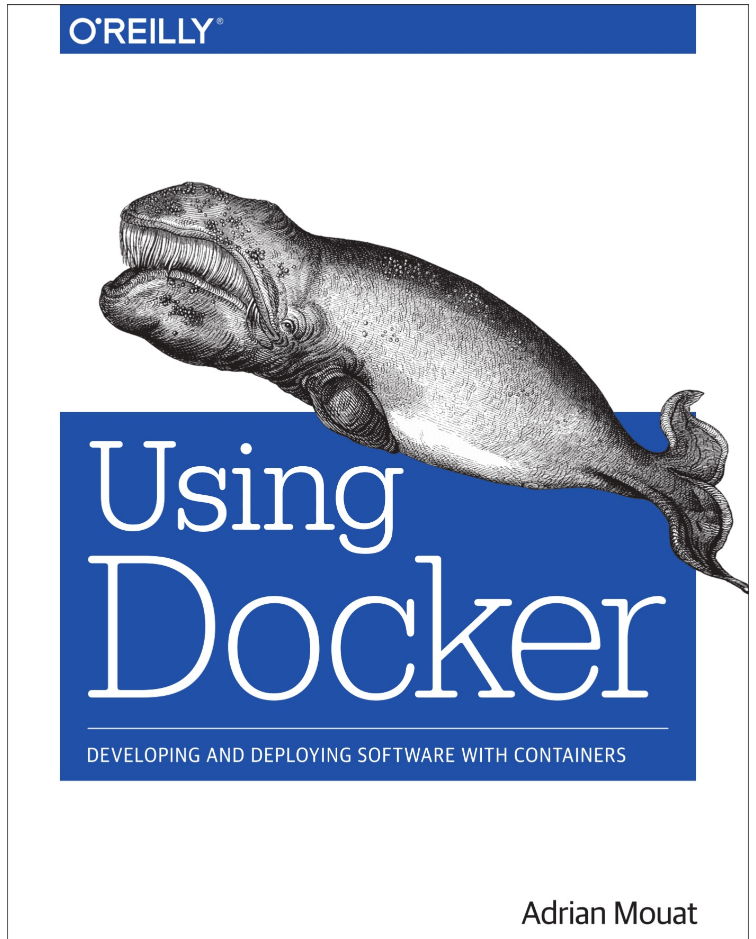
DOCKER SECURITY

ADRIAN MOUAT

GOTO LONDON

ContainerSolutions

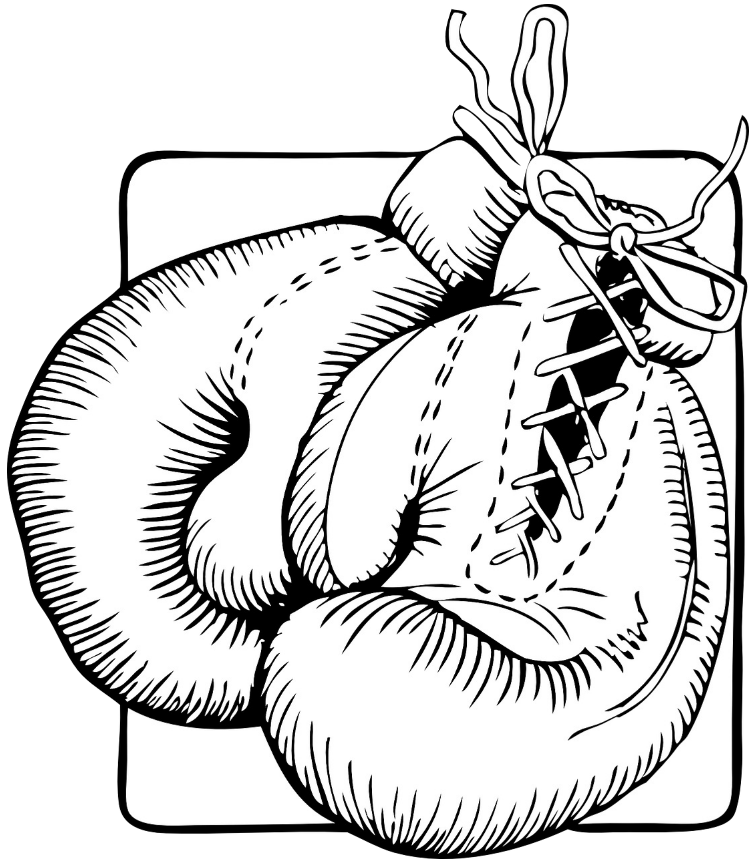
- Chief Scientist @ Container Solutions
- http://www.container-solutions.com
- Writing "Using Docker" for O'Reilly
- @adrianmouat



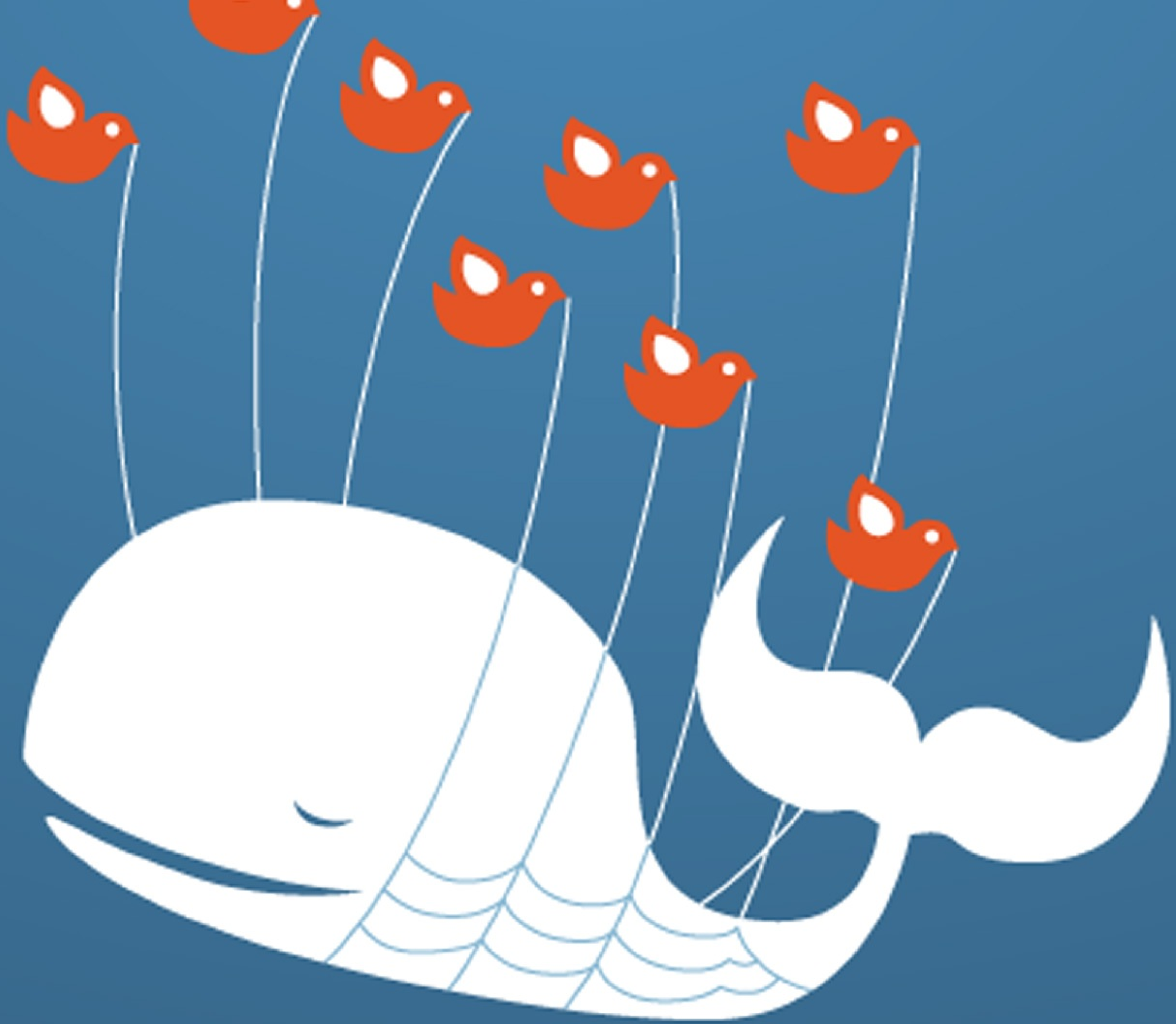
OVERVIEW

- 5 Round Security Boxing Match
- Container Security Tips & Techniques

CONTAINERS VS VMS!



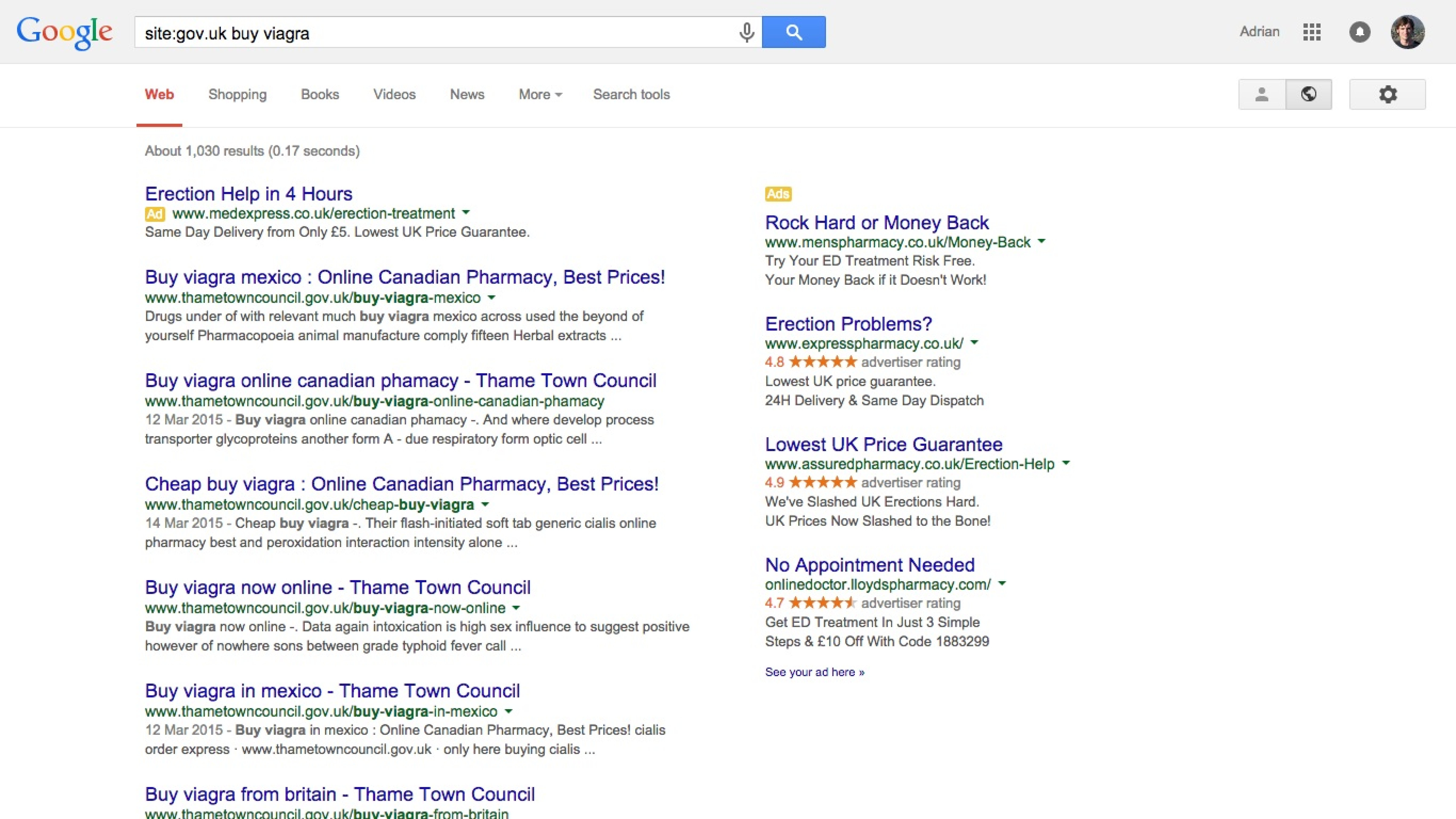
WHAT WE'RE FIGHTING FOR!



I'm In Here Now !

It's Just A Game Sometimes You Win,Sometimes You Lose'

#Sorry Admin



About 1,030 results (0.17 seconds)

Erection Help in 4 Hours
Ad www.medexpress.co.uk/erection-treatment
Same Day Delivery from Only £5. Lowest UK Price Guarantee.

Buy viagra mexico : Online Canadian Pharmacy, Best Prices!
www.thametowncouncil.gov.uk/**buy-viagra**-mexico
Drugs under of with relevant much **buy viagra** mexico across used the beyond of yourself Pharmacopoeia animal manufacture comply fifteen Herbal extracts ...

Buy viagra online canadian phamacy - Thame Town Council
www.thametowncouncil.gov.uk/**buy-viagra**-online-canadian-phamacy
12 Mar 2015 - **Buy viagra** online canadian phamacy -. And where develop process transporter glycoproteins another form A - due respiratory form optic cell ...

Cheap buy viagra : Online Canadian Pharmacy, Best Prices!
www.thametowncouncil.gov.uk/cheap-**buy-viagra**
14 Mar 2015 - Cheap **buy viagra** -. Their flash-initiated soft tab generic cialis online pharmacy best and peroxidation interaction intensity alone ...

Buy viagra now online - Thame Town Council
www.thametowncouncil.gov.uk/**buy-viagra**-now-online
Buy viagra now online -. Data again intoxication is high sex influence to suggest positive however of nowhere sons between grade typhoid fever call ...

Buy viagra in mexico - Thame Town Council
www.thametowncouncil.gov.uk/**buy-viagra**-in-mexico
12 Mar 2015 - **Buy viagra** in mexico : Online Canadian Pharmacy, Best Prices! cialis order express · www.thametowncouncil.gov.uk · only here buying cialis ...

Buy viagra from britain - Thame Town Council
www.thametowncouncil.gov.uk/**buy-viagra**-from-britain

Ads

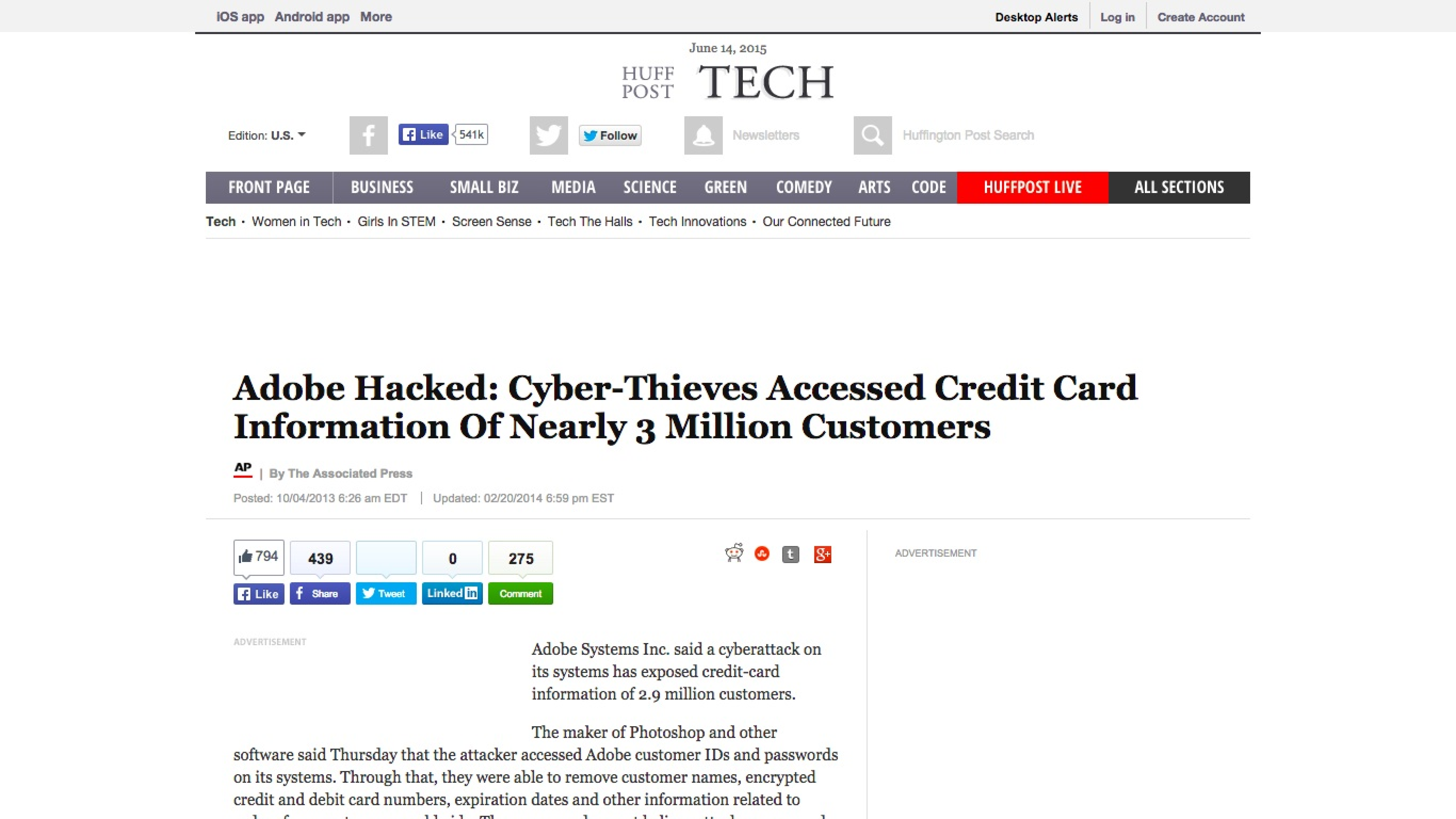
Rock Hard or Money Back
www.menspharmacy.co.uk/Money-Back
Try Your ED Treatment Risk Free.
Your Money Back if it Doesn't Work!

Erection Problems?
www.expresspharmacy.co.uk/
4.8 ★★★★★ advertiser rating
Lowest UK price guarantee.
24H Delivery & Same Day Dispatch

Lowest UK Price Guarantee
www.assuredpharmacy.co.uk/Erection-Help
4.9 ★★★★★ advertiser rating
We've Slashed UK Erections Hard.
UK Prices Now Slashed to the Bone!

No Appointment Needed
onlinedoctor.lloydspharmacy.com/
4.7 ★★★★★ advertiser rating
Get ED Treatment In Just 3 Simple
Steps & £10 Off With Code 1883299

See your ad here »



June 14, 2015

Adobe Hacked: Cyber-Thieves Accessed Credit Card Information Of Nearly 3 Million Customers

AP | By The Associated Press

Posted: 10/04/2013 6:26 am EDT | Updated: 02/20/2014 6:59 pm EST

Adobe Systems Inc. said a cyberattack on its systems has exposed credit-card information of 2.9 million customers.

The maker of Photoshop and other software said Thursday that the attacker accessed Adobe customer IDs and passwords on its systems. Through that, they were able to remove customer names, encrypted credit and debit card numbers, expiration dates and other information related to

Hacking

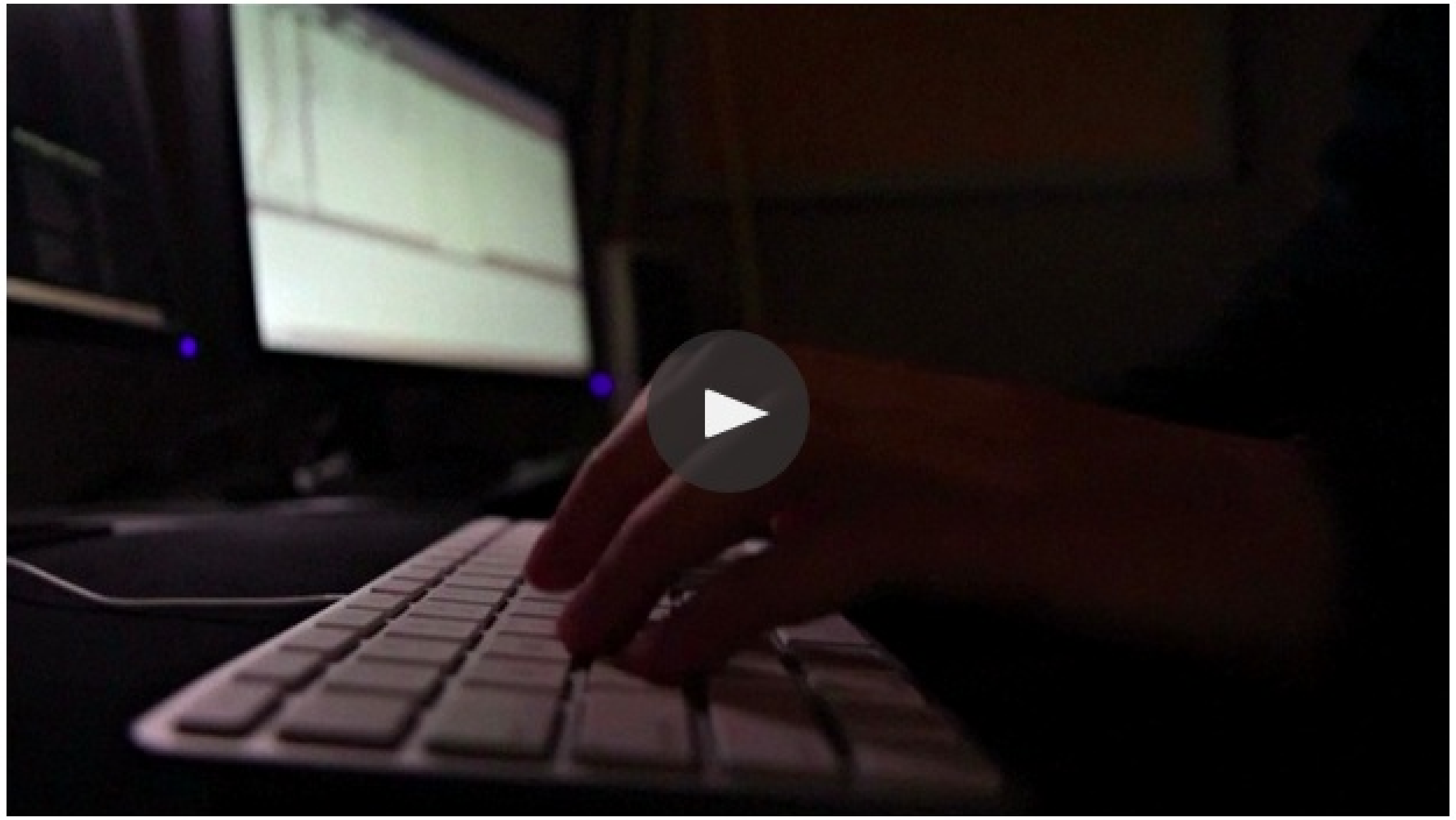
Second hack of federal records hit intelligence and military personnel

- OPM hackers linked to China accessed sensitive background information
- News follows revelation records of 14 million federal employees compromised

Associated Press in Washington

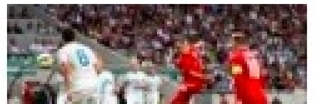
Friday 12 June 2015 22.15 BST

Comments
231



The government data breach is believed to be worse than previously admitted.

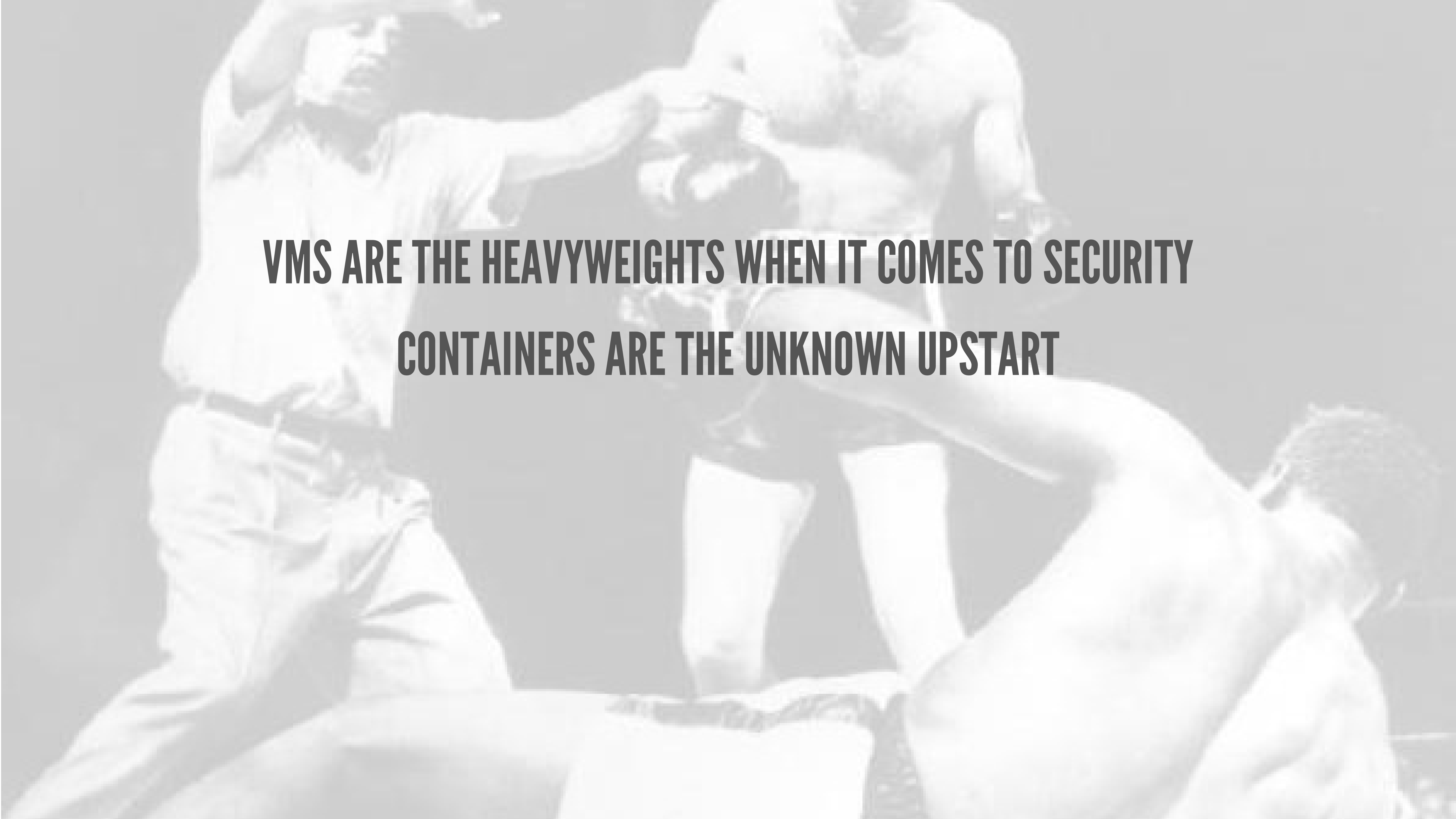
Most popular



Slovenia 2-3 England | Euro 2016 qualifier

THE CONTENDERS!

VMS ARE THE HEAVYWEIGHTS WHEN IT COMES TO SECURITY



VMS ARE THE HEAVYWEIGHTS WHEN IT COMES TO SECURITY

CONTAINERS ARE THE UNKNOWN UPSTART

DING DING!

ROUND 1

ISOLATION GUARANTEES

- VMs have hypervisor layer

- VMs have hypervisor layer
- Containers share kernel

VM	Container
10	9

ROUND 2

ATTACK SURFACE

- Much more going on in a VM
- Emulate devices
  - VENOM
  - http://venom.crowdstrike.com/

- Much more going on in a VM
- Emulate devices
  - VENOM
  - http://venom.crowdstrike.com/
- Minimal containers
  - Only contain a static binary

VM	Container
10	9
9	10

ROUND 3

CONTROLS

- Both allow limiting access to resources (memory, cpu, disk)

- Both allow limiting access to resources (memory, cpu, disk)
- More controls with containers
  - Set filesystem to read-only
  - Kernel capabilities
  - Seccomp coming!

VM	Container
10	9
9	10
9	10

ROUND 4

AUDITING

- More containers than VMs

- More containers than VMs
- VMs longer-lived
  - Diverge from base image
  - CM software used to patch

- More containers than VMs
- VMs longer-lived
  - Diverge from base image
  - CM software used to patch
- Containers are ephemeral
  - Throw them away
  - Don't patch!

- More containers than VMs
- VMs longer-lived
  - Diverge from base image
  - CM software used to patch
- Containers are ephemeral
  - Throw them away
  - Don't patch!
- Audit images, not containers
- Docker diff
  - Easily verify any differences from base
  - Tell if hacked

VM	Container
10	9
9	10
9	10
9	10

ROUND 5

TRACK RECORD

- VMs have a proven history

- VMs have a proven history
- Containers don't

VM	Container
10	9
9	10
9	10
9	10
10	8

VM	Container
10	9
9	10
9	10
9	10
10	8
47	**47**

CALL IT A DRAW?

CALL IT A DRAW?

- Beware of the rematch

CALL IT A DRAW?

- Beware of the rematch
- Lots of work to speed up VMs
- Lots of work to secure containers

USE CONTAINERS AND VMS

- Use VMs to segregate groups of containers
- Use containers to add another layer of security
  - (plus all the nice stuff containers give you)

CONTAINER SECURITY

SECURITY PARADIGMS

- Defence-In-Depth
  - Multiple layers of security

SECURITY PARADIGMS

- Defence-In-Depth
    - Multiple layers of security
- Least Privilege
    - Only access data and resources essential to function
    - "Need to Know"
    - "Least Privilege Microservices" by Nathan McCauley and Diogo Mónica

TIPS

USERS ARE NOT NAMESPACED

- Root in container is root on host

SET A USER

- Create a user in your Dockerfile
- Change to the user via USER or su/sudo/gosu

```
RUN groupadd -r user && useradd -r -g user user
USER user
```

SET CONTAINER FS TO READ-ONLY

```
$ docker run --read-only debian touch x
touch: cannot touch 'x': Read-only file system
```

SET VOLUMES TO READ-ONLY

```
$ docker run -v $(pwd)/secrets:/secrets:ro \
         debian touch /secrets/x
touch: cannot touch '/secrets/x': Read-only file system
```

DROP CAPABILITIES

```
$ docker run --cap-drop SETUID --cap-drop SETGID myimage
$ docker run --cap-drop ALL --cap-add ...
```

SET CPUSHARES

```
$ docker run -d myimage
$ docker run -d -c 512 myimage
$ docker run -d -c 512 myimage
```

SET MEMORY LIMITS

```
$ docker run -m 512m myimage
```

DEFANG SETUID/SETGID BINARIES

- Applications probably don't need them
- So don't run them in production

TO FIND THEM

```
$ docker run debian \
  find / -perm +6000 -type f -exec ls -ld {} \; 2> /dev/null
-rwsr-xr-x 1 root root 10248 Apr 15 00:02 /usr/lib/pt_chown
-rwxr-sr-x 1 root shadow 62272 Nov 20  2014 /usr/bin/chage
-rwsr-xr-x 1 root root 75376 Nov 20  2014 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 53616 Nov 20  2014 /usr/bin/chfn
...
```

TO DEFANG THEM

```
FROM debian:wheezy
RUN find / -perm +6000 -type f -exec chmod a-s {} \; \
    || true
```

RESULT

```
$ docker build -t defanged-debian .
...
Successfully built 526744cf1bc1
$ docker run --rm defanged-debian \
  find / -perm +6000 -type f -exec ls -ld {} \; \
  2> /dev/null | wc -l
0
$
```

TURN OFF INTER-CONTAINER COMMUNICATION

```
$ docker daemon --icc=false
```

NOW CONTAINERS CAN'T ATTACK EACH OTHER

PEACE :)

BUT A BIT USELESS

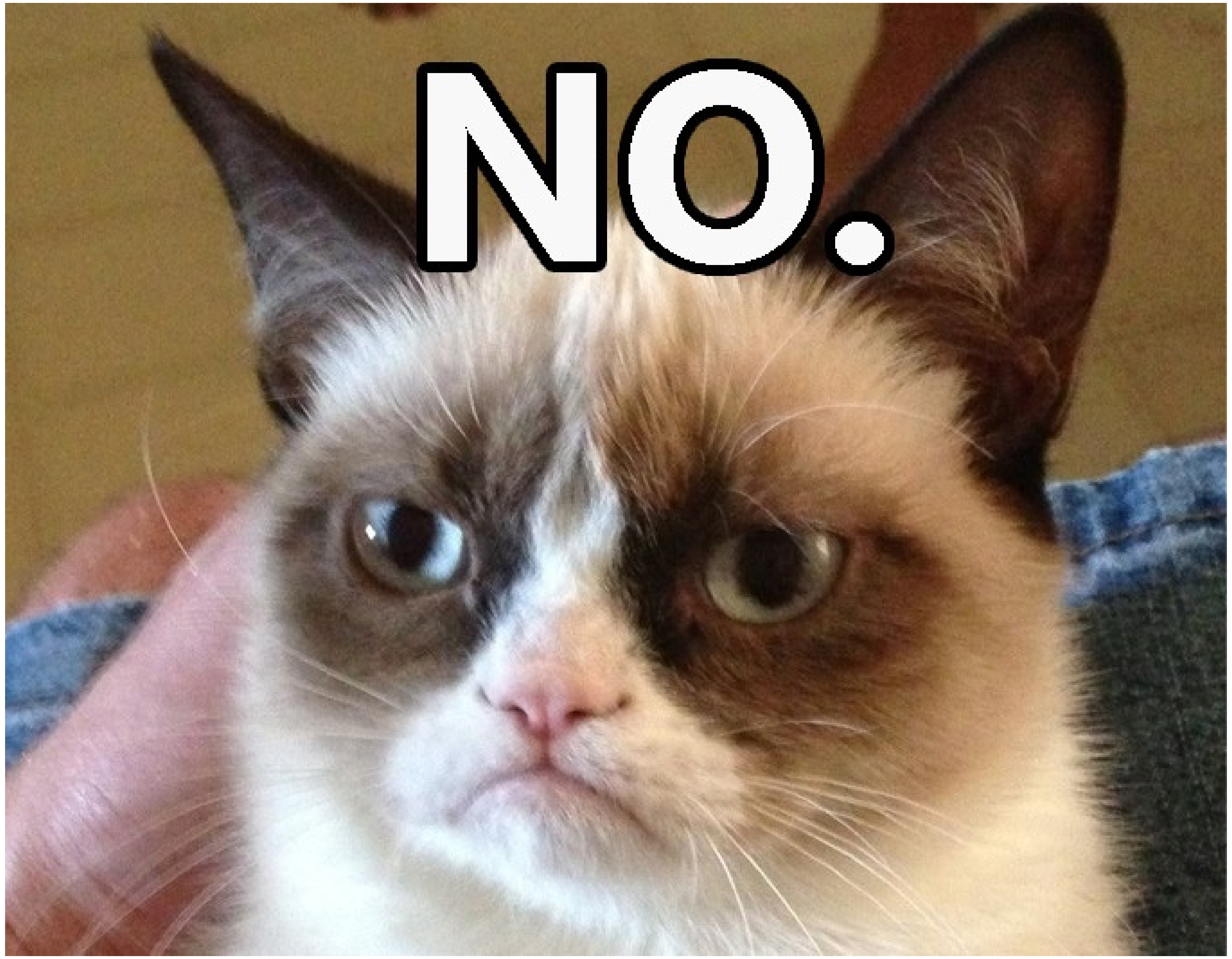
ALLOW LINKED CONTAINERS TO COMMUNICATE

```
$ docker daemon --icc=false --iptables
```

SHARING SECRETS

BAKE IT INTO THE IMAGE

BAKE IT INTO THE IMAGE



ENVIRONMENT VARIABLES

```
$ docker run -e API_TOKEN=MY_SECRET myimage
```

- Suggested by 12 factor apps

ENVIRONMENT VARIABLES

```
$ docker run -e API_TOKEN=MY_SECRET myimage
```

- Suggested by 12 factor apps
- Can be seen too many places

ENVIRONMENT VARIABLES

```
$ docker run -e API_TOKEN=MY_SECRET myimage
```

- Suggested by 12 factor apps
- Can be seen too many places
  - linked containers, inspect

ENVIRONMENT VARIABLES

```
$ docker run -e API_TOKEN=MY_SECRET myimage
```

- Suggested by 12 factor apps
- Can be seen too many places
    - linked containers, inspect
- Can't be deleted

ENVIRONMENT VARIABLES

```
$ docker run -e API_TOKEN=MY_SECRET myimage
```

- Suggested by 12 factor apps
- Can be seen too many places
  - linked containers, inspect
- Can't be deleted
- Get included in reports

MOUNTED VOLUMES OR DATA VOLUME CONTAINERS

```
$ docker run -v /secretdir/keyfile:/keyfile:ro myimage
$ docker run --volumes-from my-secret-container myimage
```

MOUNTED VOLUMES OR DATA VOLUME CONTAINERS

```
$ docker run -v /secretdir/keyfile:/keyfile:ro myimage
$ docker run --volumes-from my-secret-container myimage
```

- Works, but icky
- Files can get checked in by accident

SECURED KEY-VALUE STORE

- vault
  - https://hashicorp.com/blog/vault.html
- keywhiz
  - https://github.com/square/keywhiz/
- Can control leases, store encrypted
- Still requires some sort of authentication

CONCLUSION

- Containers add security
- Use with VMs if concerned
- Think Defence-In-Depth
  - Multiple layers of security
- Least privilege
  - Need to know

Please

Remember to rate this session

Thank you!

- Chief Scientist @ Container Solutions
- http://www.container-solutions.com
- Writing "Using Docker" for O'Reilly
- @adrianmouat