

SECURITY AT SCALE



Davi Ottenheimer
@daviottenheimer
Boston, April 2014

Edward H. Adelson



© Copyright 2014 EMC Corporation. All rights reserved.

WHOAMI



2014 Breach Analysis: flyingpenguin

"While high flying speeds can be detrimental to landing on tree perches for flying birds, there is little consequence to high impact landing in water."

@daviottenheimer

- 🔒 Anthropology of Language / Music / Math
"Shintiri: the secret language"
- 🔒 Bike / Sailboat Racing
- 🔒 Ethics of "Humanitarian Intervention"
- 🔒 International History
- 🔒 ...& 20 Years InfoSec



© Blophoto / Christopher Swann



EMC²

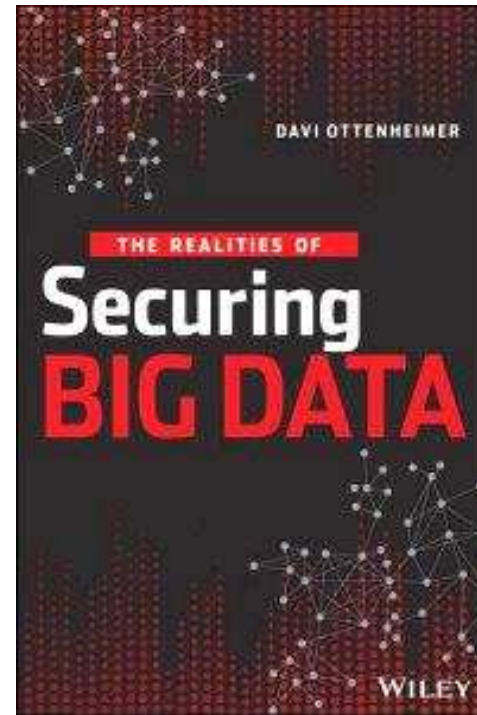
Pivotal

RSA

vmware



GROWING BODY OF DATA OBESITY RESEARCH



EMC²

Pivotal



vmware[™]



RESEARCHING...



the grugq
@thegrugq

Slides for my talk on mobile phone operational security and hardening Android: slideshare.net/grugq/mobile-o... + source code: github.com/grugq/darkmatt...

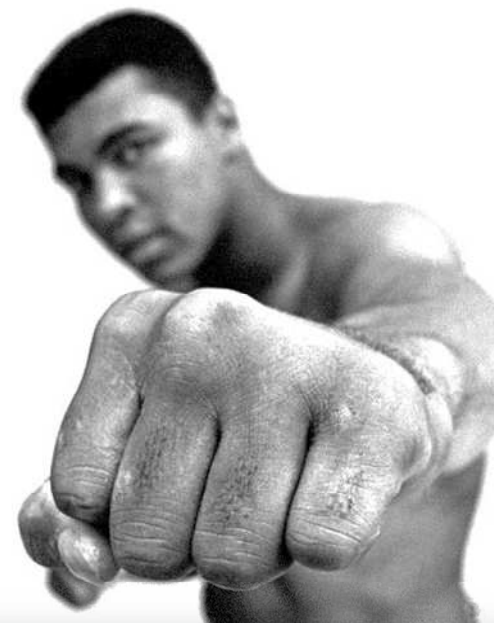
↩ Reply ↻ Retweeted ★ Favorite ⋮ More

RETWEETS
139

FAVORITES
177



2:23 AM - 4 Apr 2014



“If you want to lose a fight, talk about it first”

–Quellcrist Falconer



EMC²

Pivotal

RSA

vmware



RESEARCHING...

<http://www.twitter.com/thegrugq/status/452013704632991745>

“If you want to lose a fight, talk about it first”

–Quellcrist Falconer

W http://en.wikipedia.org/wiki/Quellcrist_Falconer

If you want to lose a fight, talk about it first.

Furies



Woken Furies

By Richard K. Morgan

If you want to lose a fight

Go

No results found in this book f



Woken Furies

By Richard K. Morgan

http://books.google.com/books?id=RvJMkL8cuw0C&pg=PA138&ots=9_MMVQdOcP&dq=quellcrist%20falconer%20%20woken%20furies&pg=PA138#v=snippet&q=If%20you%20want%20to%20lose%20a%20fight,%20talk%20about%20it%20first&f=false

st - Search all books »



EMC²

Pivotal



vmware



DEFENSE RESEARCH

DETECTION

AVOIDANCE



EMC²

Pivotal

RSA

vmware[™]



CONTINUOUS AVAILABILITY / DATA PROTECTION

AVOIDANCE

<http://www.emc.com/collateral/demos/microsites/mediaplayer-video/continuous-operations-oracle-rac-emc-vplex.htm>



EMC²

Pivotal



vmware[™]



A person wearing a black balaclava and a red jacket is standing in a garage. The background shows a white garage door, a bicycle, and various tools and equipment hanging from the ceiling. The word "DETECTION" is overlaid in large white letters with a black outline.

DETECTION

CAUGHT ON TAPE

VACATIONING COUPLE THWART BURGLAR

PHONE APP HELPS CATCH CROOK

DEFENSE RESEARCH

KNOWLEDGE

PRIVACY



EMC²

Pivotal



vmware[™]



KNOWLEDGE



EMC²

Pivotal

RSA

vmware[®]





GNAWLEDGE



EMC²

Pivotal



vmware[™]



<http://compass.ups.com/UPS-driver-avoid-left-turns/>

NO LEFT
TURN
IDLING



EMC²

Pivotal



vmware[™]

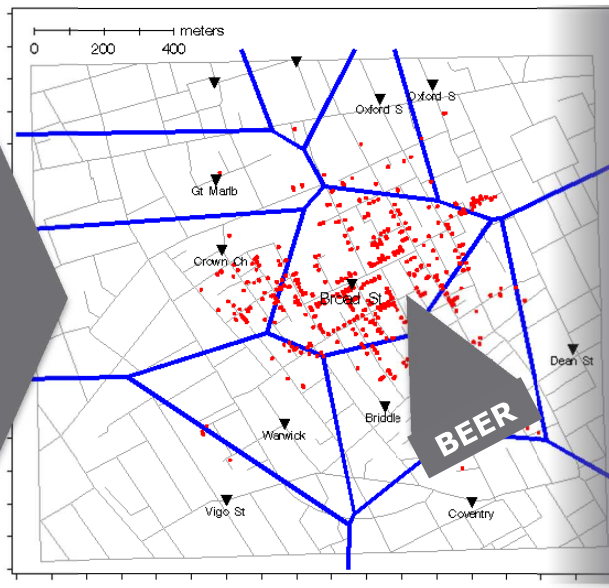


LESSONS FROM THE SNOW DEN

1854: GHOST MAP OF LONDON

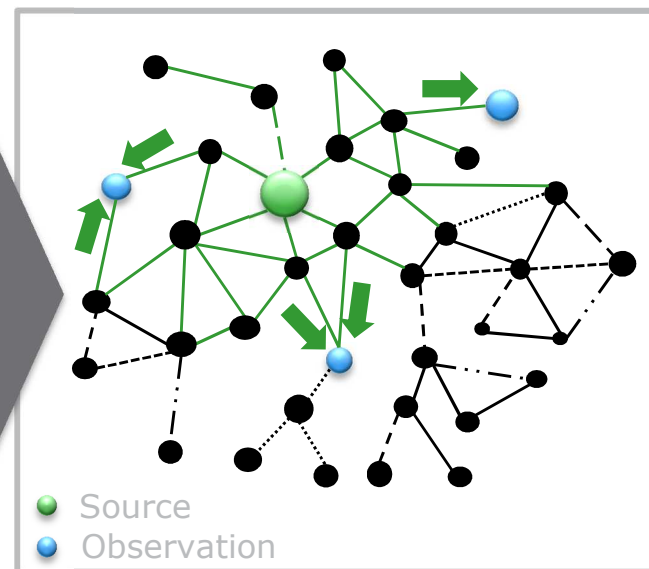


1854: CHOLERA VORONOI



(2010 Rinderpest, 2013 AIDS)

RSAC 2012: BREACH DATA

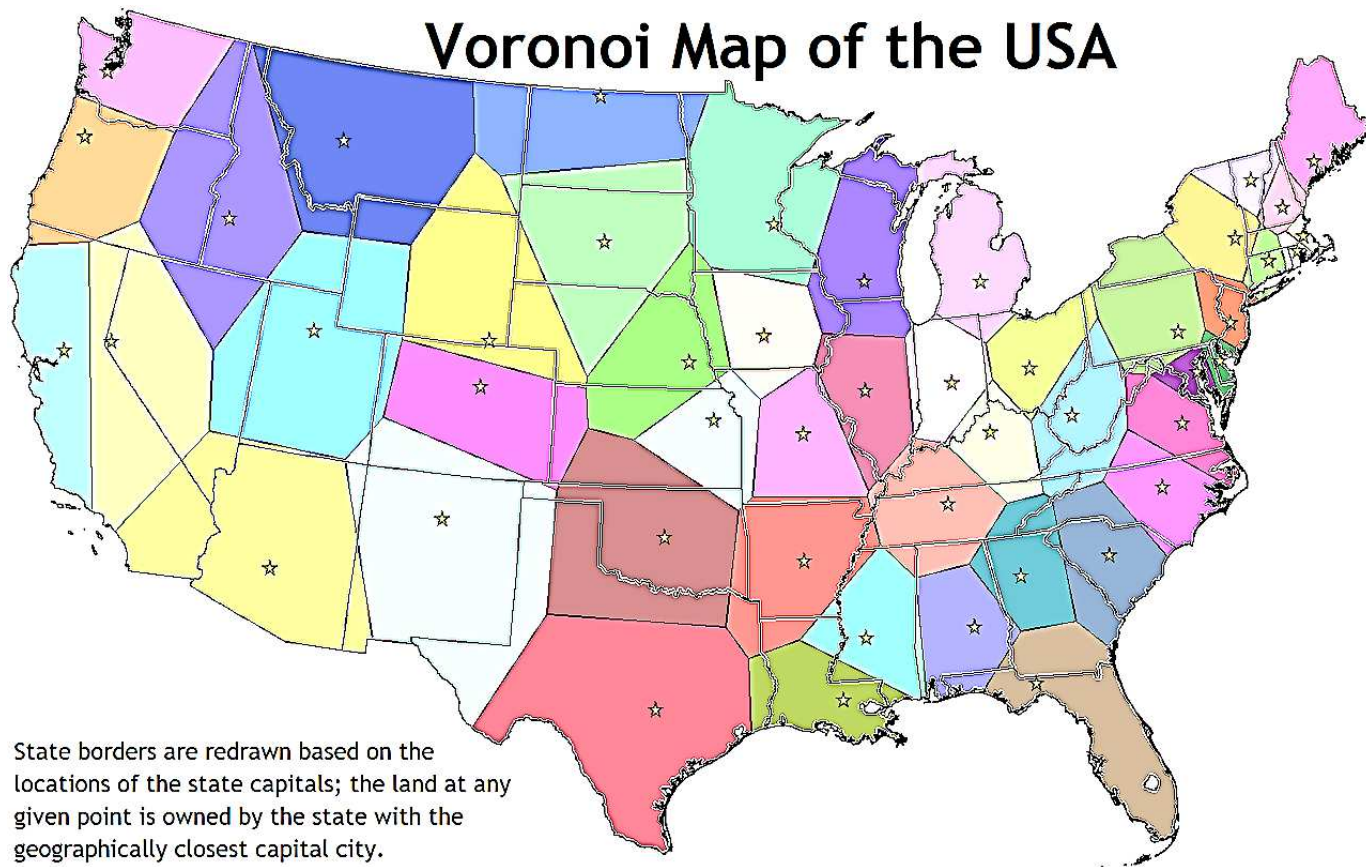


<http://www.flyingpenguin.com/?p=18259>

John Snow
1813-1858

FURTHEST POINT FROM POLITICIANS

Voronoi Map of the USA



State borders are redrawn based on the locations of the state capitals; the land at any given point is owned by the state with the geographically closest capital city.

<http://vizual-statistix.tumblr.com/post/48625446909/these-are-voronoi-maps-of-the-contiguous-usa>



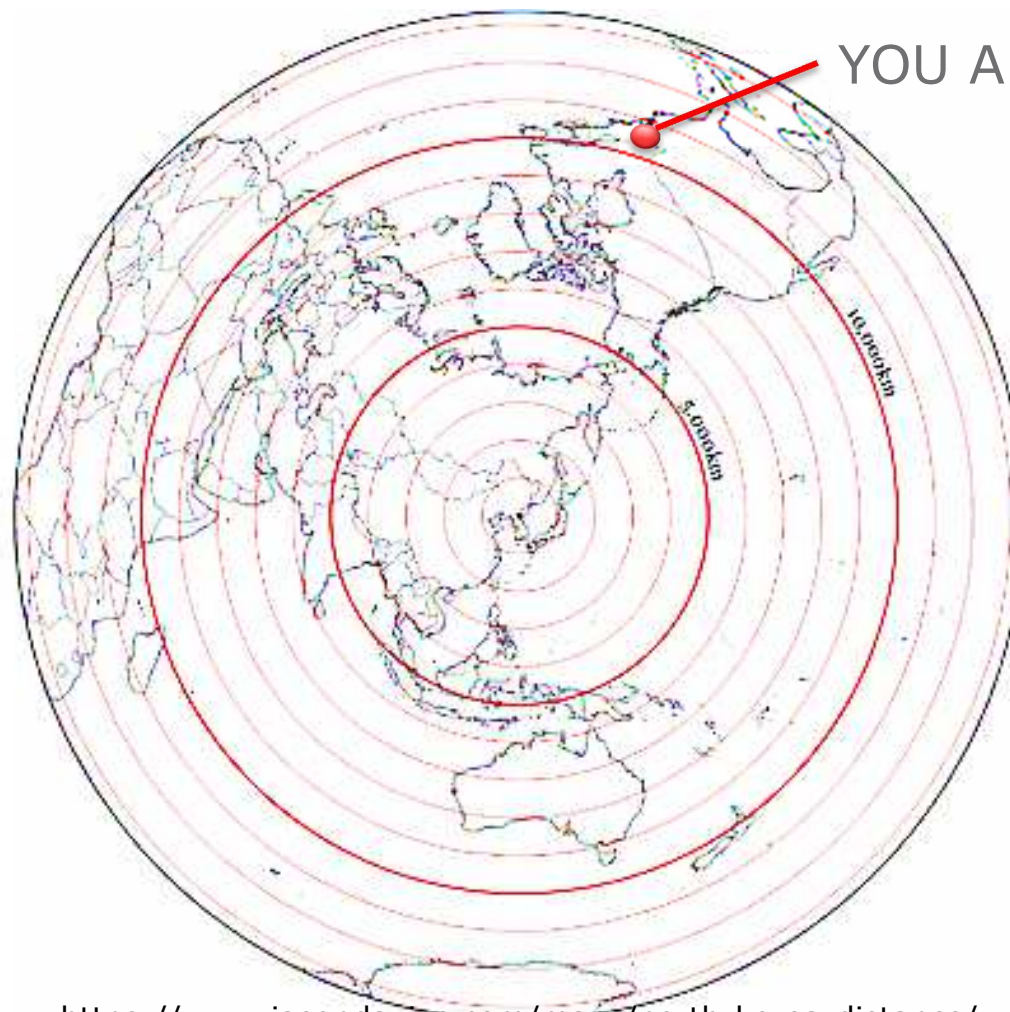
EMC²

Pivotal



vmware





YOU ARE HERE

<https://www.jasondavies.com/maps/north-korea-distance/>



EMC²

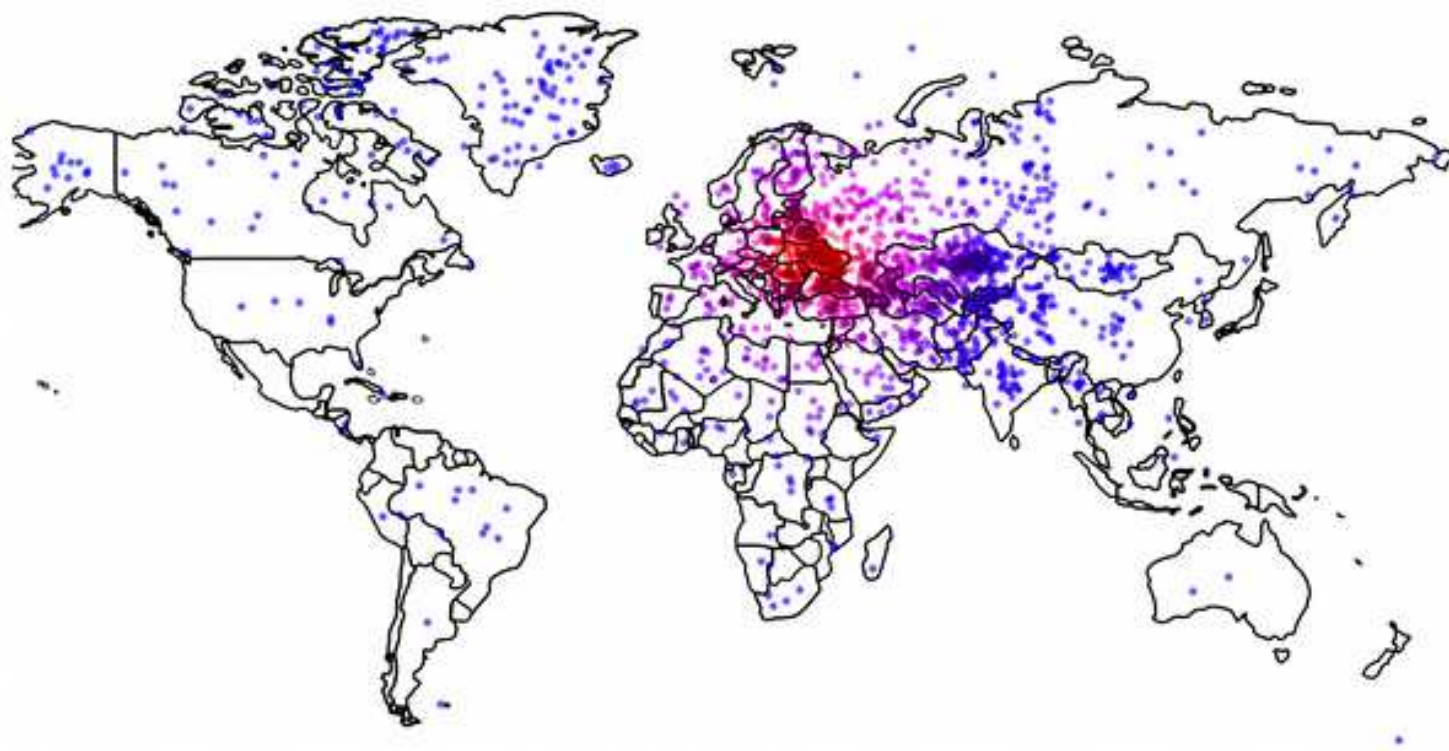
Pivotal



vmware[®]



“THE LESS AMERICANS KNOW...THE MORE THEY WANT TO INTERVENE”



Where's Ukraine? Each dot depicts the location where a U.S. survey respondent situated Ukraine; the dots are colored based on how far removed they are from the actual country, with the most accurate responses in red and the least accurate ones in blue. (Data: Survey Sampling International; Figure: Thomas Zeitzoff/The Monkey Cage)

<http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/04/07/the-less-americans-know-about-ukraines-location-the-more-they-want-u-s-to-intervene/>



EMC²

Pivotal



vmware



SOME F'ING HARD PUZZLES AHEAD

FINISHED FILES ARE THE RESULT OF YEARS OF SCIENTIFIC STUDY COMBINED WITH THE EXPERIENCE OF YEARS...



EMC²

Pivotal

RSA

vmware[™]



KNOWLEDGE




EMC²

Pivotal

RSA

vmware[™]





Give me six hours to chop
down a tree and I will
spend the first four
sharpening the axe.

Quellcrist Falconer

GNAWLEDGE

"COWS NOT PETS"



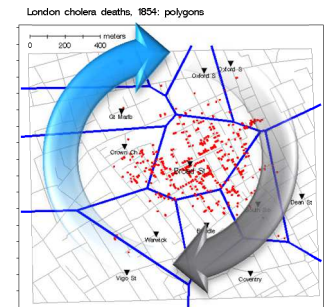
Systematic Treatment of Illness

Easily Identified

Routine Treatment

Minimum Judgment

- I**dentify Sickness ASAP
- K**eep Adequate Records
- E**valuate Daily Sick
- A**dapt Until Noted Improvement



EMC²

Pivotal

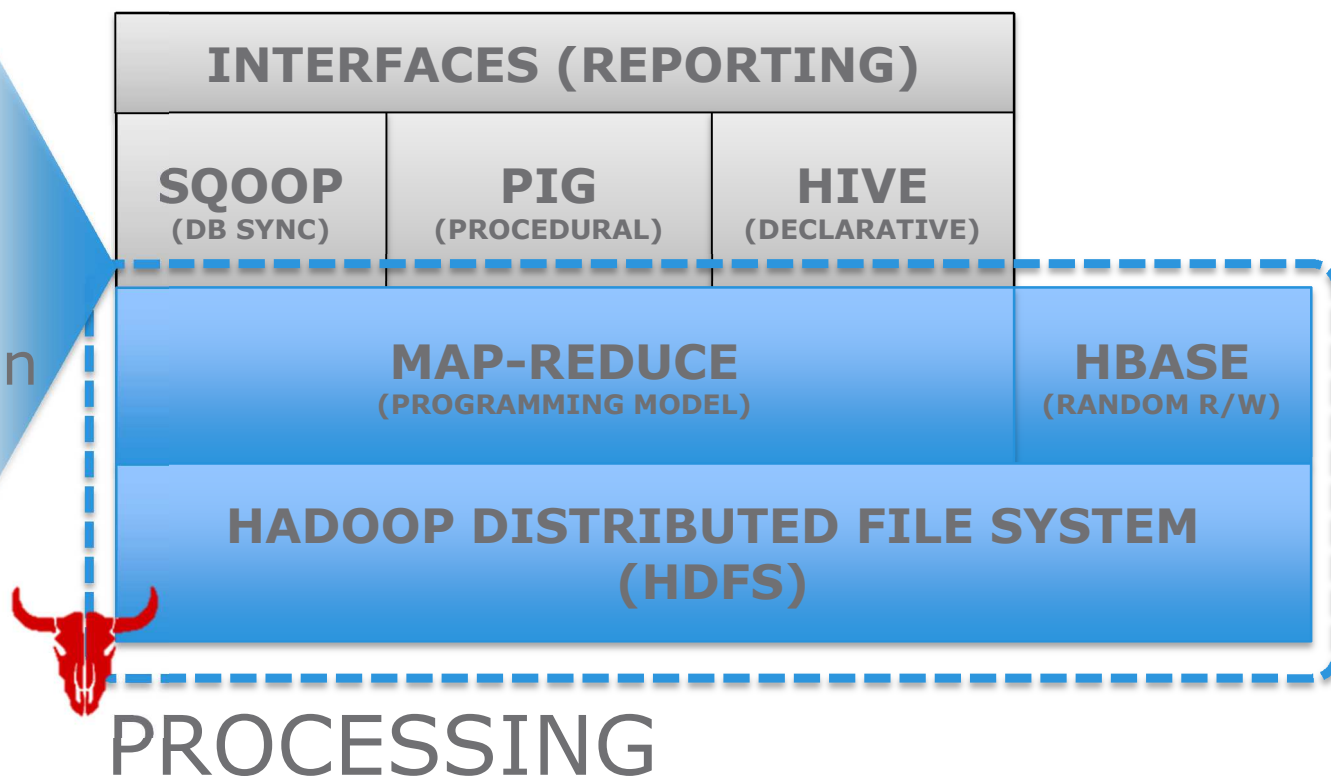


vmware

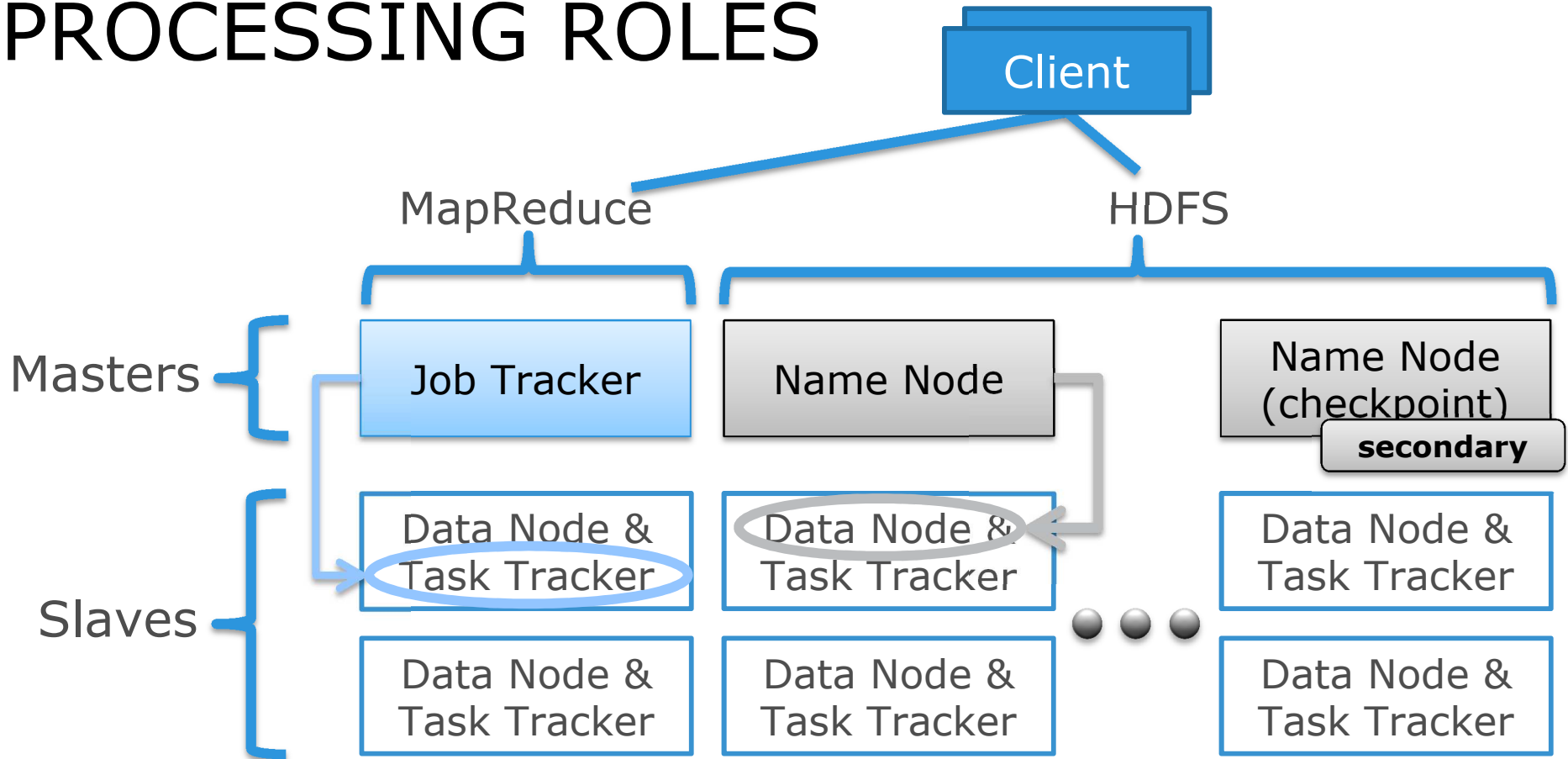


EARLY DATA ARCHITECTURE AND CONTROL

- Data Shared
- Nodes Distributed
- Clients Unauthenticated
- Access Controls Open
- Web Services Open
- Networks Open



PROCESSING ROLES



EMC²

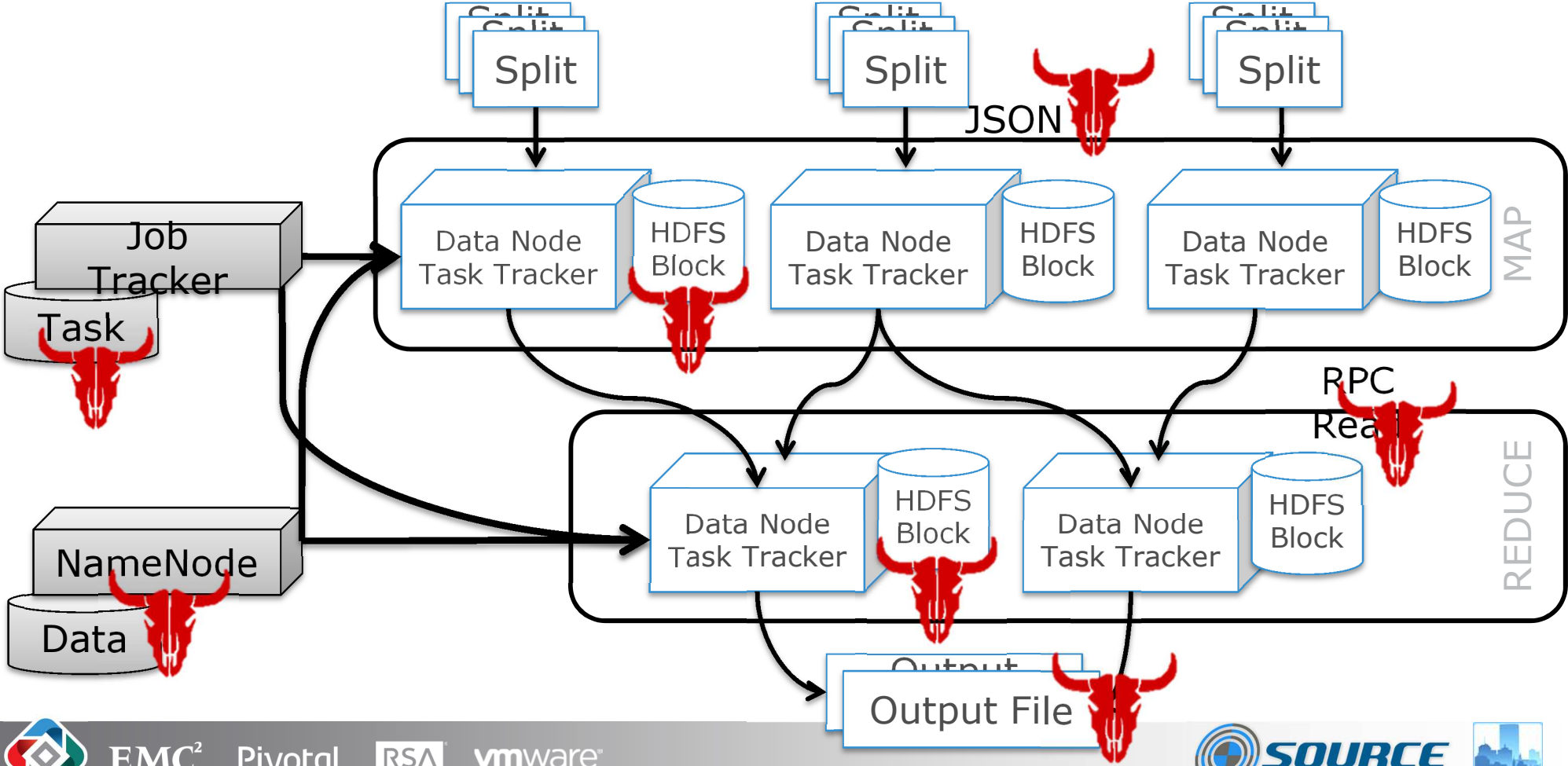
Pivotal



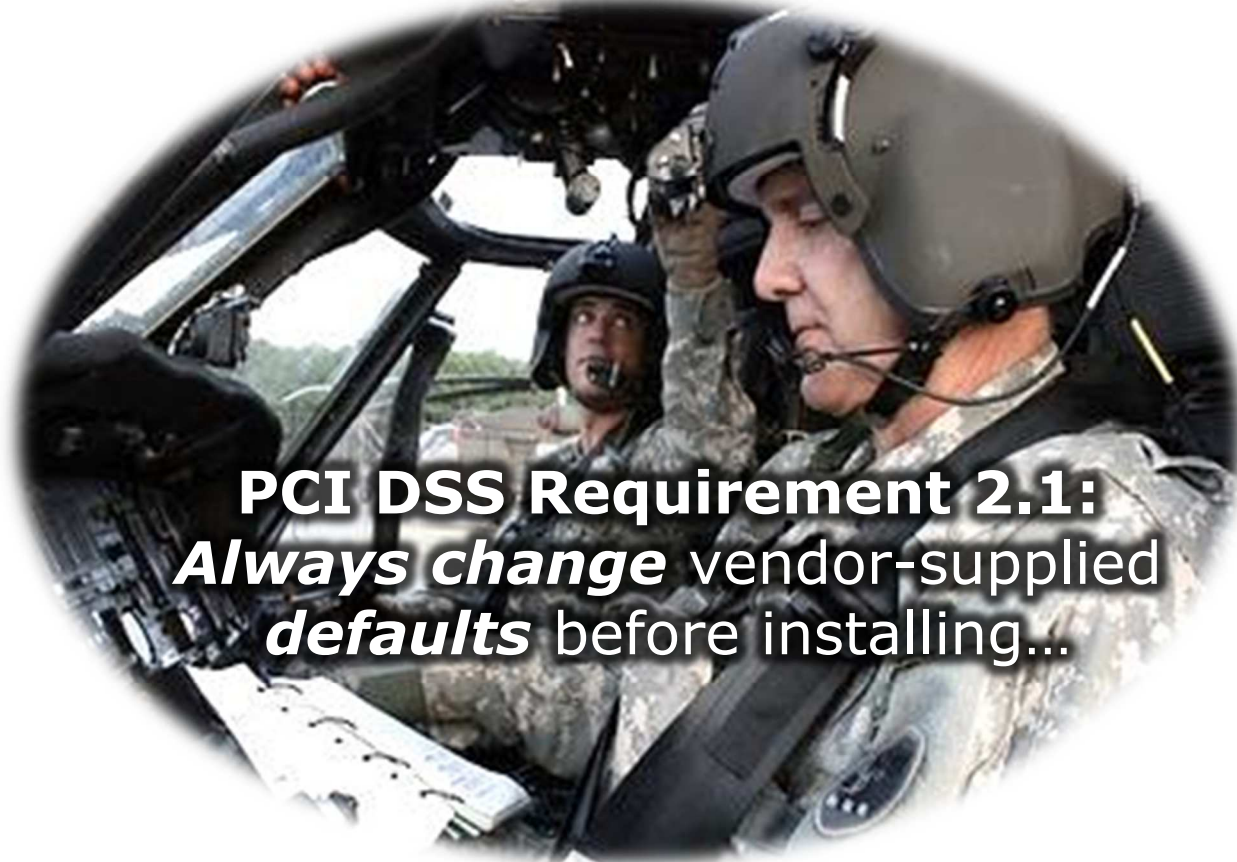
vmware



PROCESSING PATHS



"SIMPLE" CHECKLISTS



PCI DSS Requirement 2.1:
Always change vendor-supplied
defaults before installing...



http://www.mdjonline.com/view/full_story/9738998/article-Father-trains-son--to-fly-helicopters-with-night-vision
<http://www.dvidshub.net/image/962244/oklahoma-national-guard-pilots-train-war-time-standard>



EMC²

Pivotal



vmware[®]



INTELLIGENT ANALYSIS AT SCALE

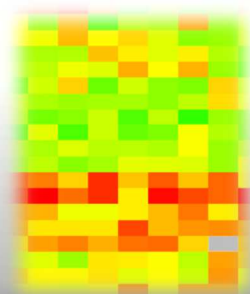
BINARY



RANKED



MEANING



ZERO
POINT



EXACT



ERROR MARGIN

INTELLIGENCE

CAVEAT: "NO FISH IN TOO CLEAR WATER"



EMC²

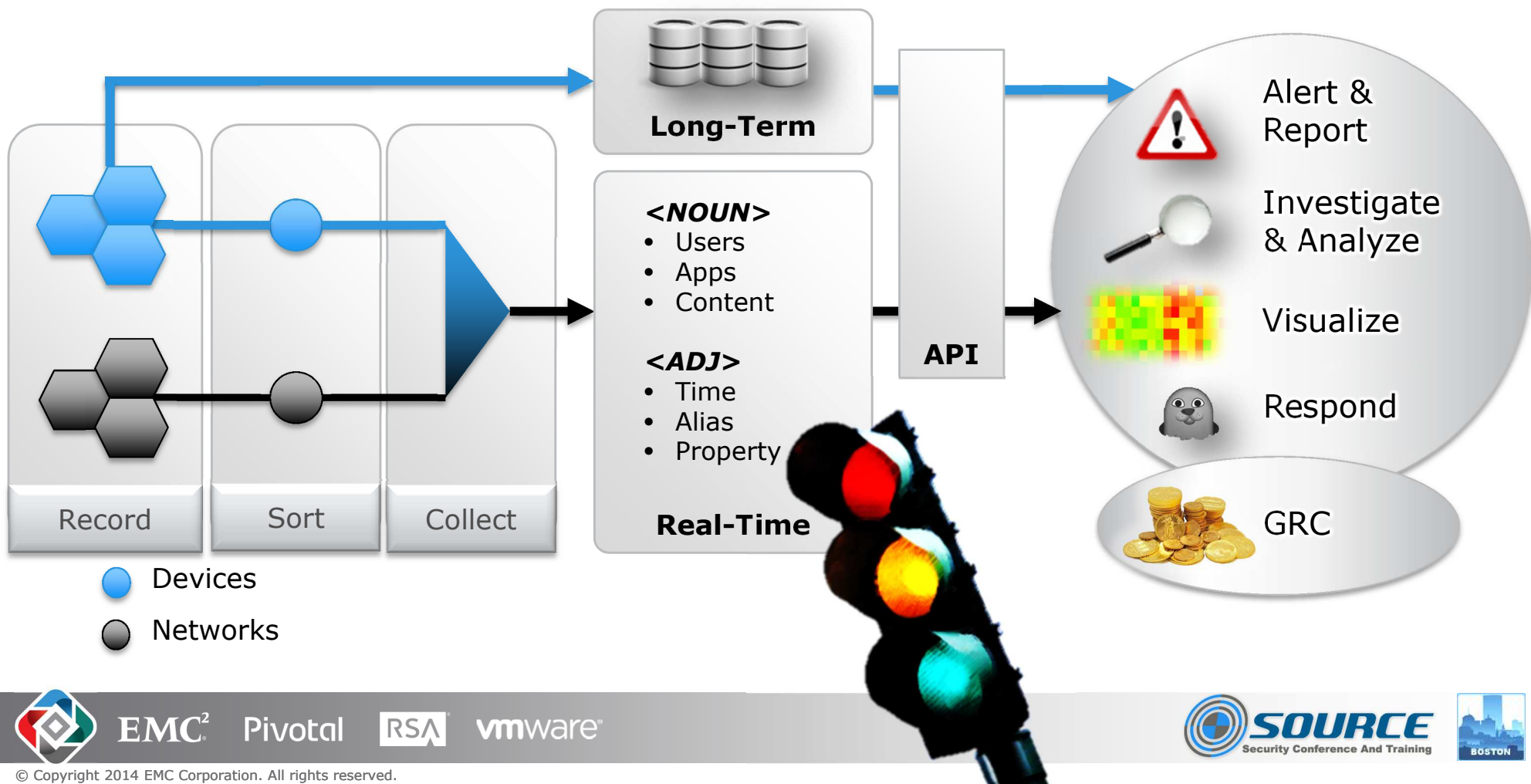
Pivotal



vmware[™]



INTELLIGENCE REDEFINES CONTROLS



INTELLIGENT CONTROLS AT SCALE

Annual Savings

- 33 Years of Time
- US\$8,000,000
- 27 Fuel Tanker Trucks



<http://rhythmttraffic.com/insyncs-performance/>



© Copyright 2014 EMC Corporation. All rights reserved.

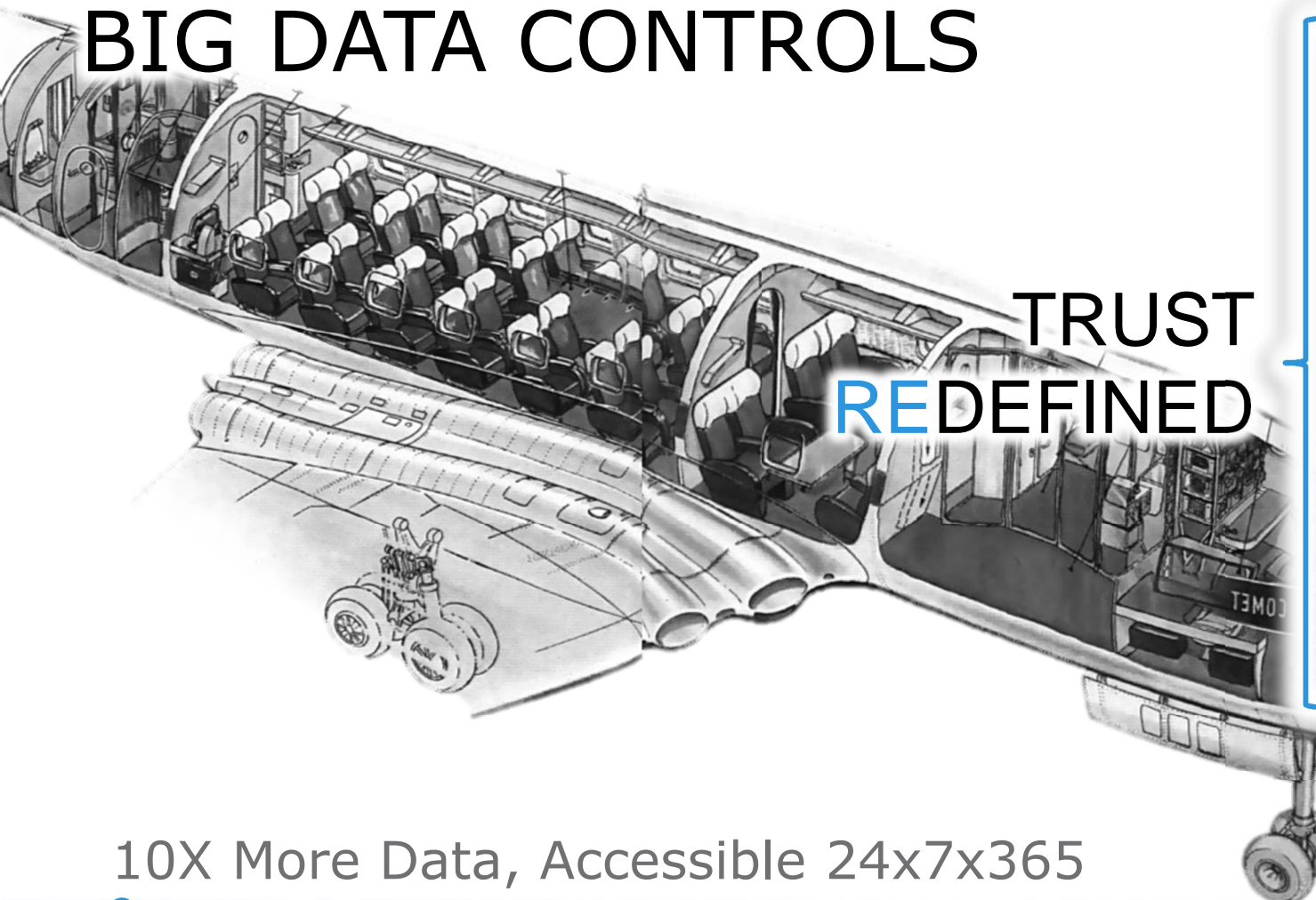


DATA CONTROLS



- Brakes
- Suspension
- Horn
- Mirrors
- Seatbelts

BIG DATA CONTROLS



TRUST
REDEFINED

- ~~Brakes~~
- ~~Suspension~~
- ~~Horn~~
- ~~Mirrors~~
- Seatbelts
- Checklists
- Threat Avoidance

10X More Data, Accessible 24x7x365



EMC²

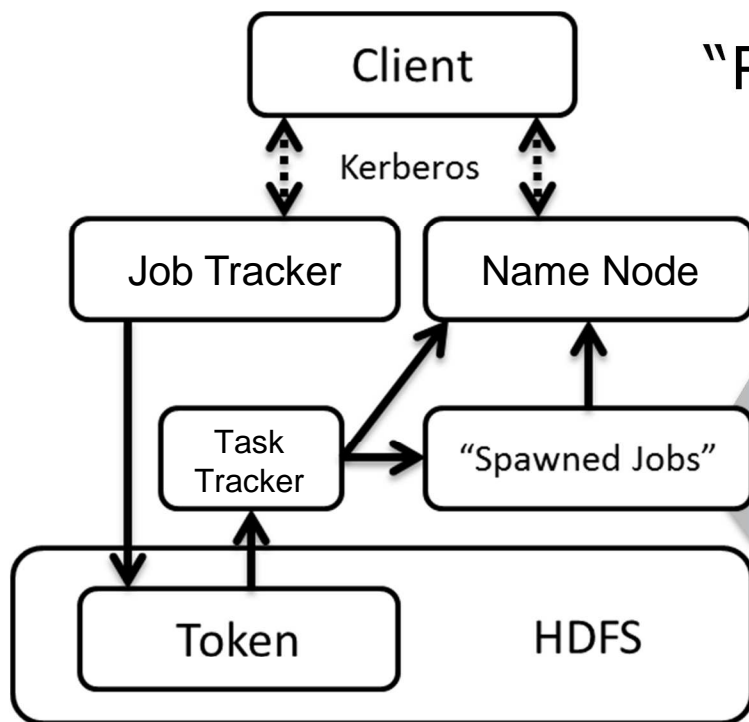
Pivotal



vmware[®]



BEWARE TRUST DELEGATIONS



"Runaway Job! Kill -9"



PRIVACY

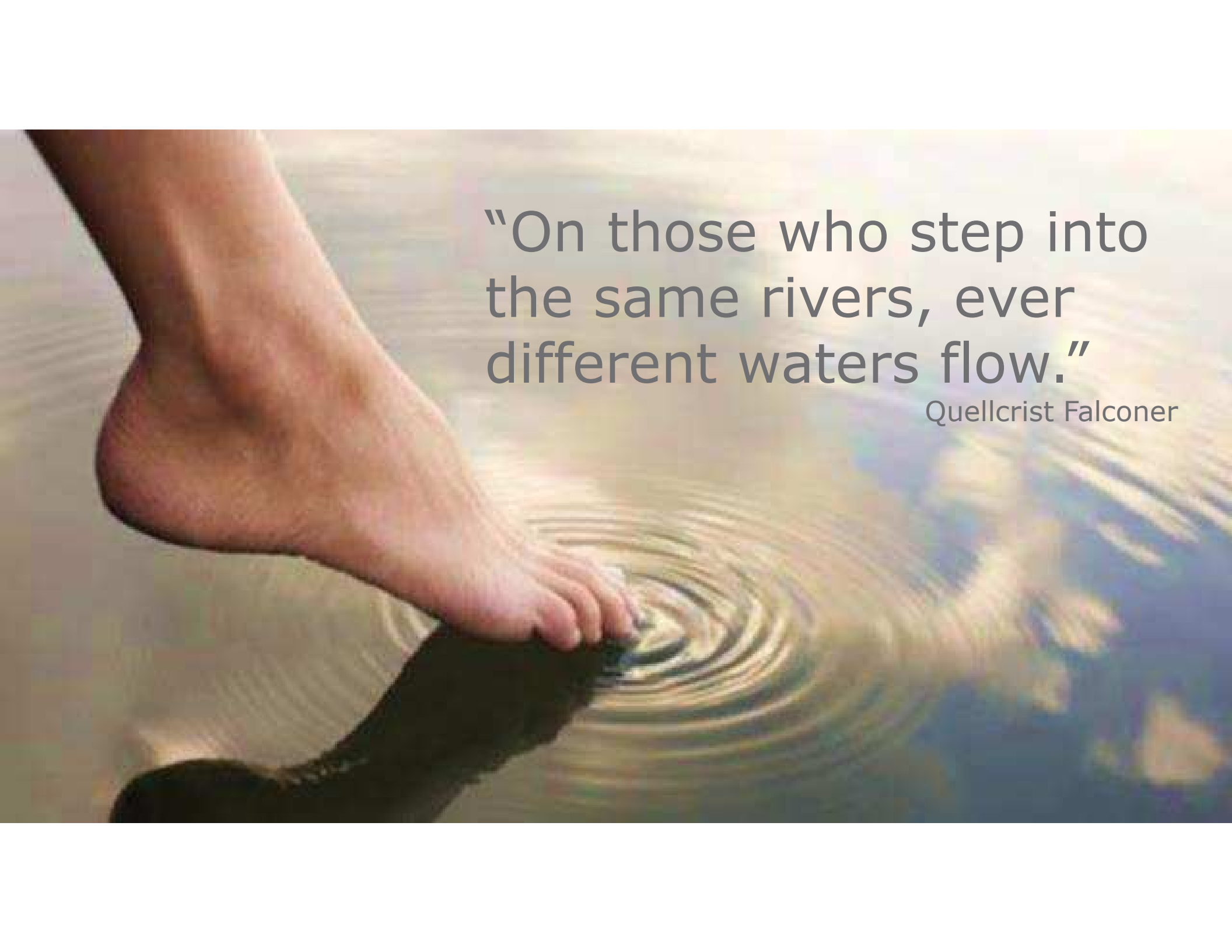


EMC²

Pivotal



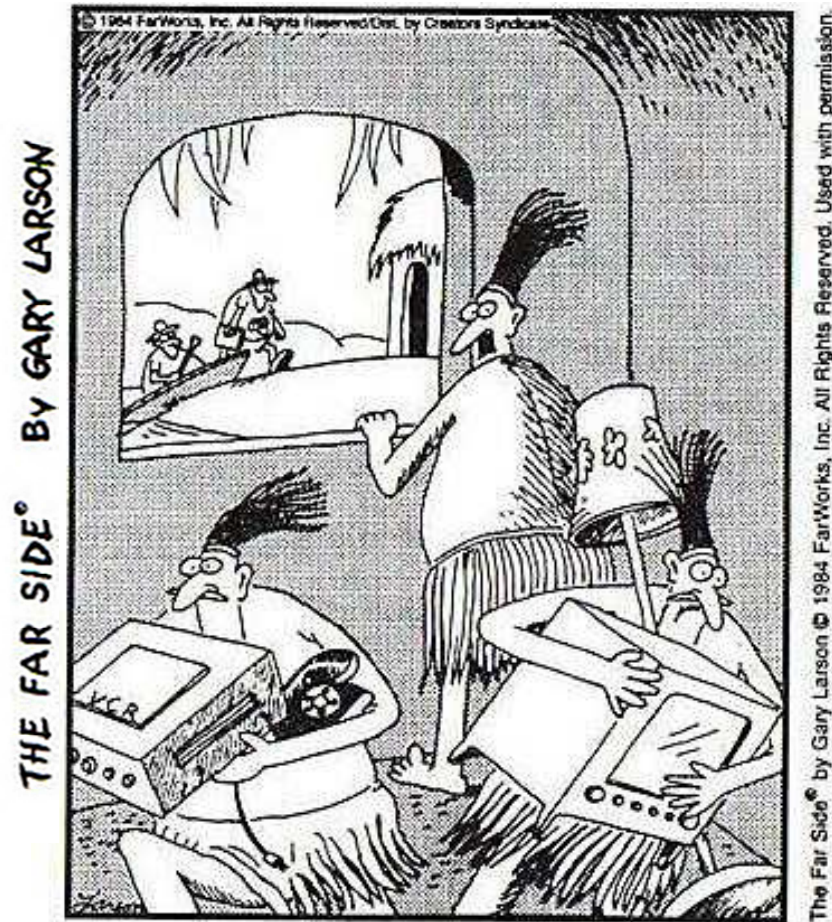
vmware[®]



“On those who step into
the same rivers, ever
different waters flow.”

Quellcrist Falconer

Anthropologists! Anthropologists!



EMC²

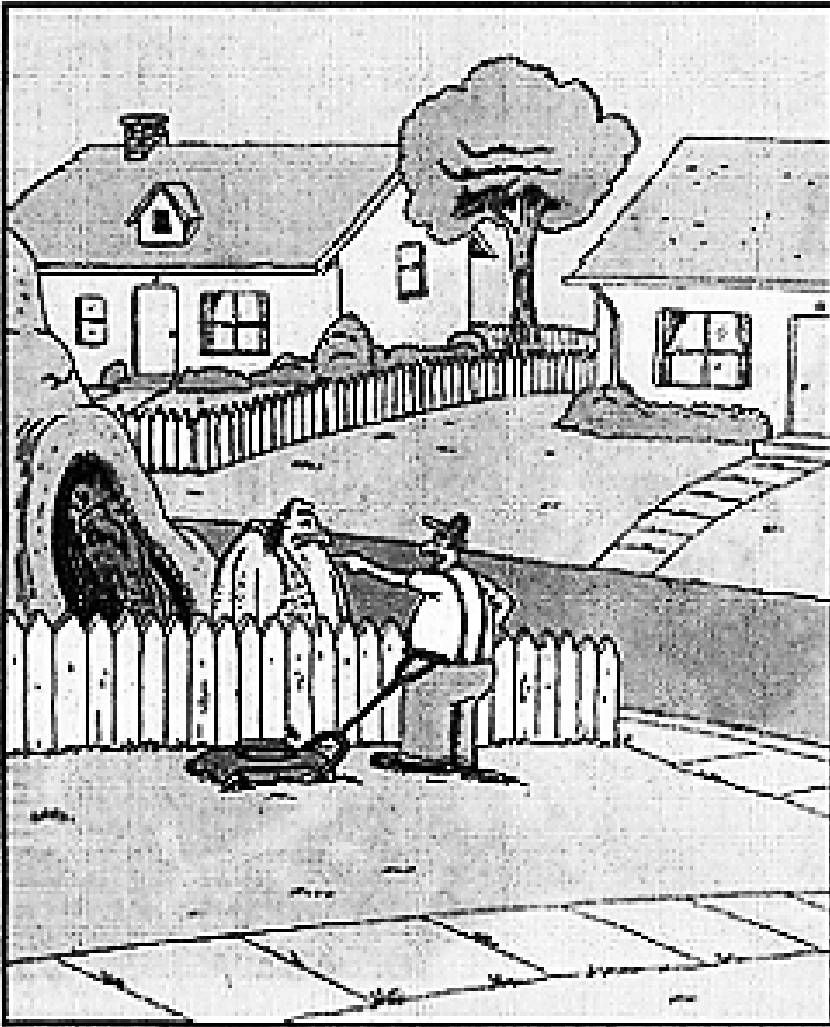
Pivotal



vmware



THE FAR SIDE® BY GARY LARSON



For The New York Times

© 1998 The Woods, Inc. The Far Side®

Don't threaten me,
Thagerson!

My cousin's an
anthropologist and
she can make your
life hell!



EMC² Pivotal RSA vmware



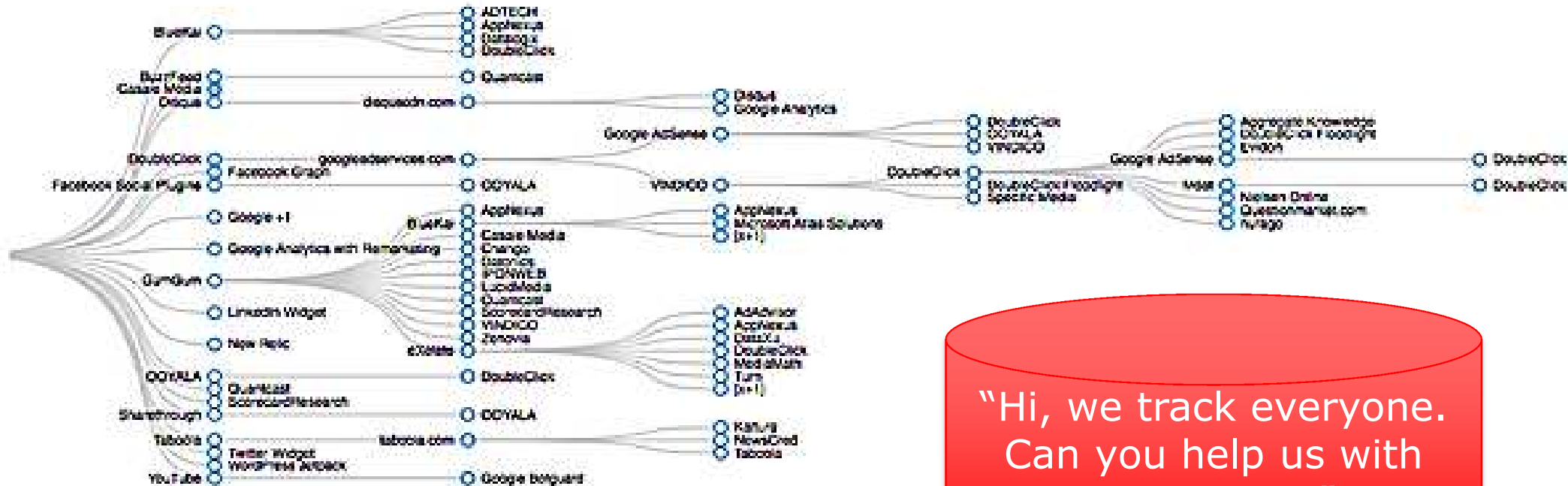
REAL-TIME ARCHAEOLOGY



<http://gizmodo.com/meth-in-london-heroin-in-zagreb-the-answer-is-found-i-1508209127>

ONE CLICK

GOOGLE SPOOKS ARE ON YOUR TAIL!



https://twitter.com/jason_kint/status/451716219482025984/photo/1

“Hi, we track everyone. Can you help us with ISO27001?”





ONE CLICK

“**Ad blocking** to me is so fundamentally wrong, it just boils my blood... fundamental **threat** that it is.”

General Counsel and EVP Public Policy

Interactive Advertising Bureau

“We Googled my name, and up popped an ad suggesting I had an arrest record. I do not.”

<http://phys.org/news/2013-05-fairness-ads-outlines-bias-score.html>

<http://www.cnet.com/news/ad-blockers-get-ad-group-execs-blood-boiling-q-a/>



EMC²

Pivotal



vmware[™]



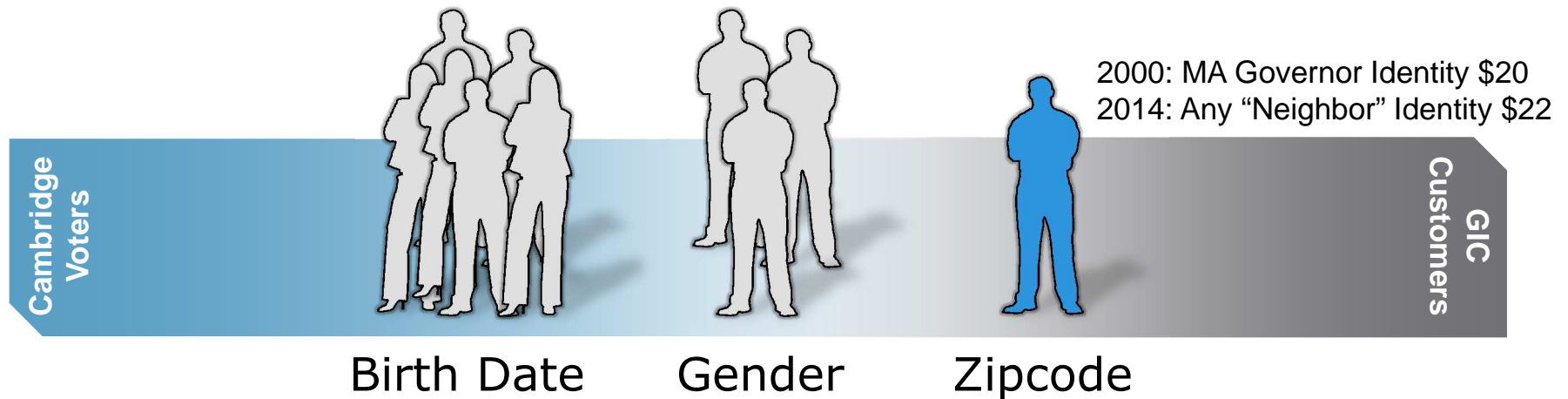
RE-IDENTIFICATION

- 53% IDs Unique
DOB + Sex + City
- 87% IDs Unique
DOB + Sex + Zip
- State/Year
Minimum Advised

“Few Characteristics Needed”

Latanya Sweeney, 2000

RE-IDENTIFICATION



Voter Registration / Group Insurance Commission (GIC) Data

<http://dataprivacylab.org/projects/identifiability/index.html>
<http://www.uclalawreview.org/?p=1353>
<http://www.zeit.de/2014/07/harald-martenstein-datenschutz>



EMC²

Pivotal

RSA

vmware[™]



PRIVACY



EMC²

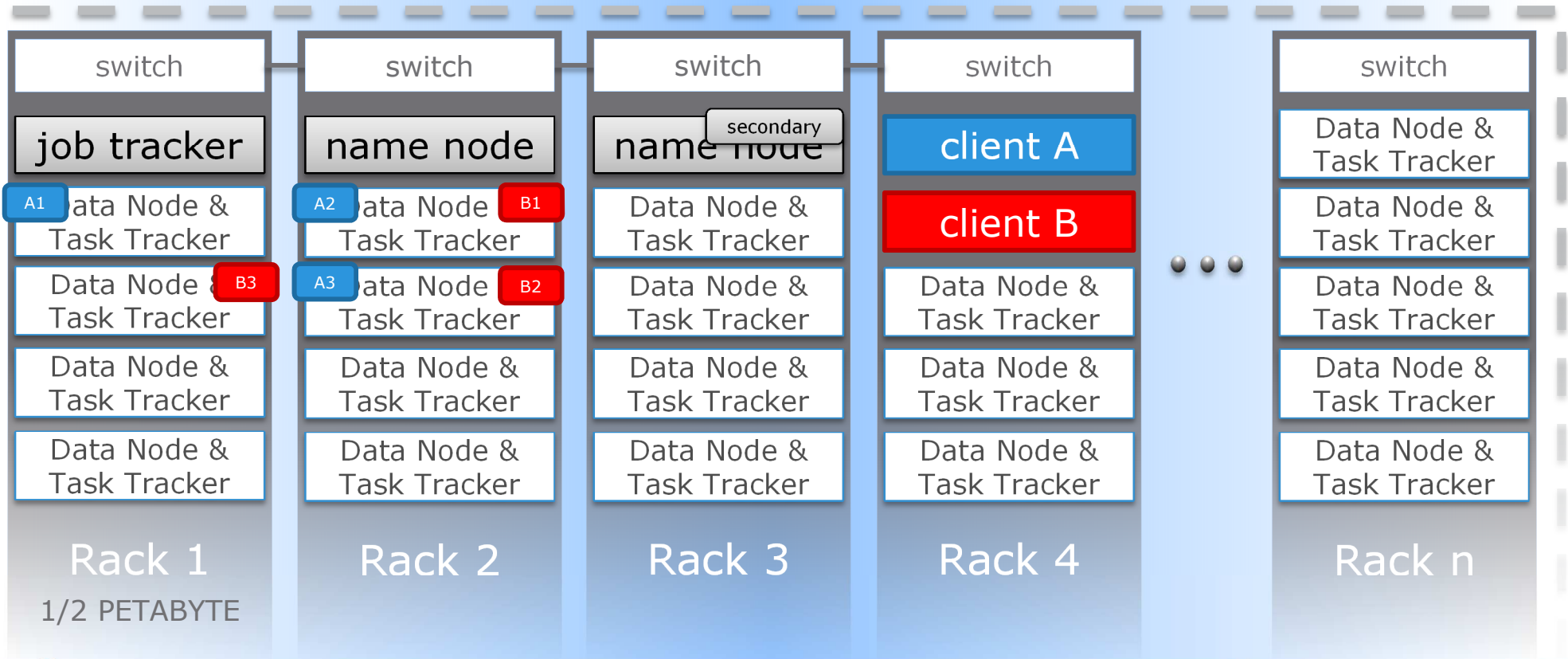
Pivotal



vmware[®]

1 Admin : 30,000+ Nodes

EARLY HADOOP ARCHITECTURE



EMC²

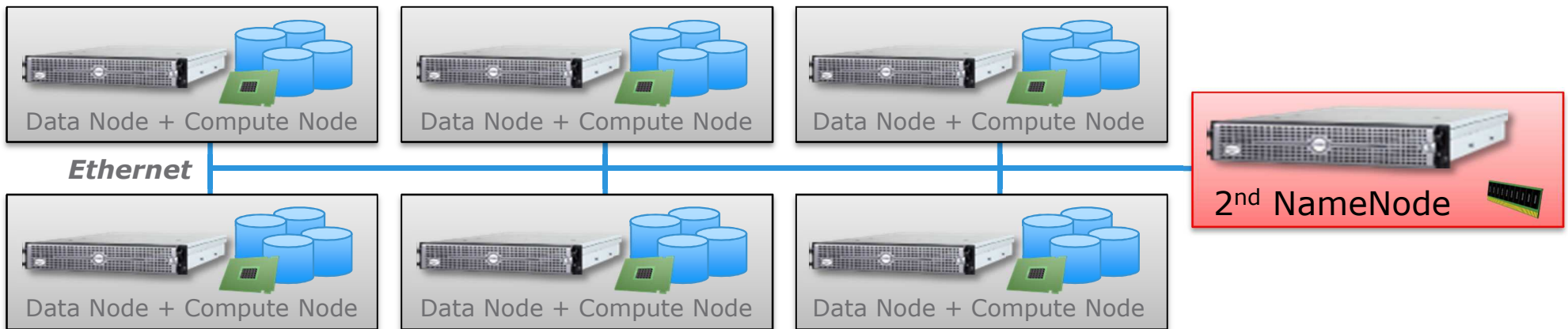
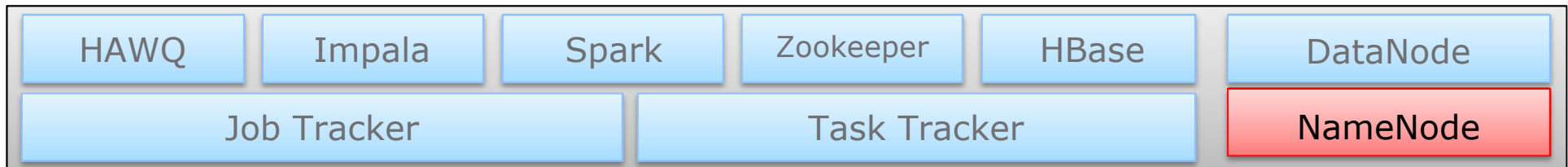
Pivotal



vmware[®]



EARLY HADOOP ARCHITECTURE



EMC²

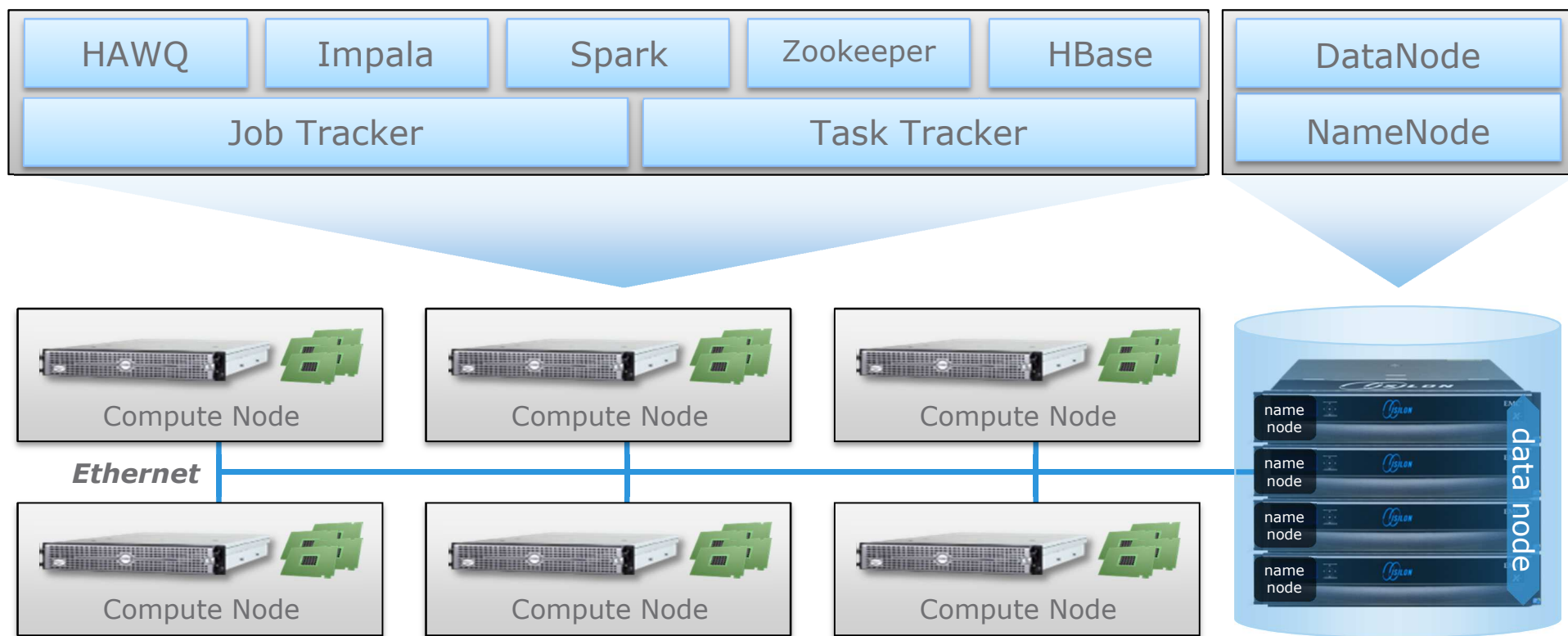
Pivotal



vmware[™]



MODERN HADOOP ARCHITECTURE



EMC²

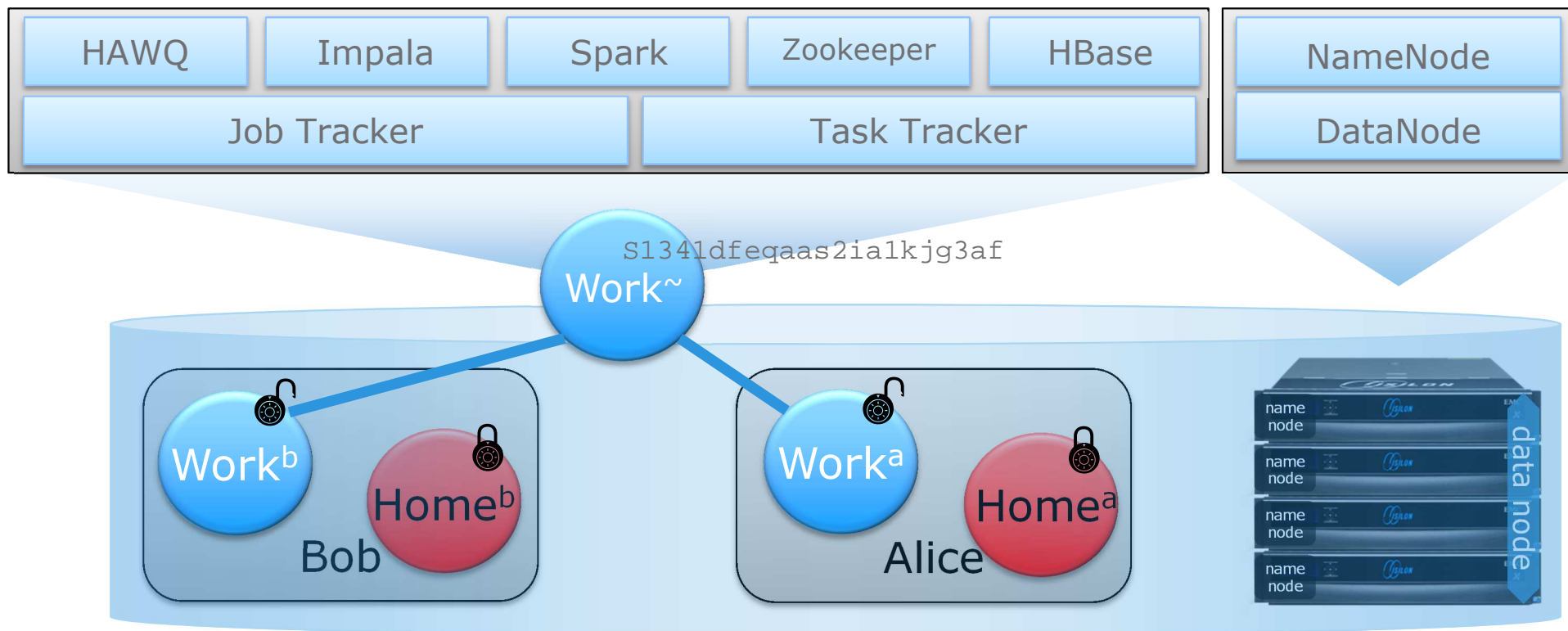
Pivotal



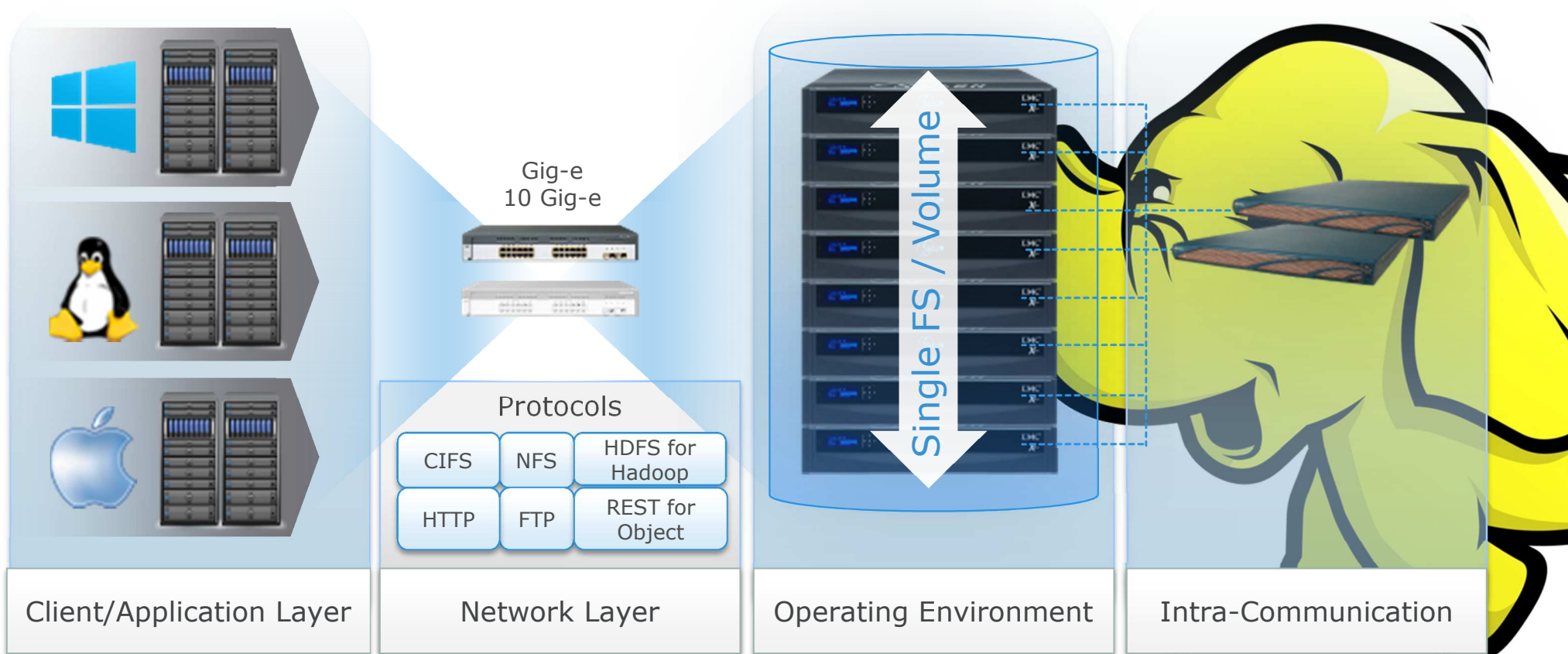
vmware[™]



ACCESS BY AUTHORITY



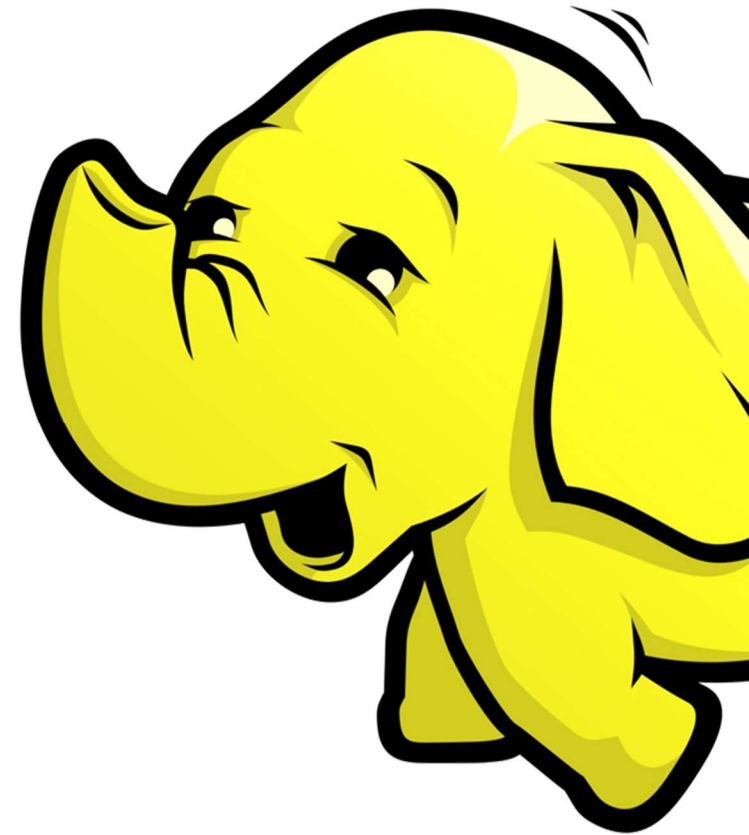
SCALE-OUT CONTROL ARCHITECTURE



CONTROLS AT SCALE

Trusted Big Data

- Full ACLs on File Systems
- Multi-Tenancy Aware
- Kerberos Authentication
- High-Resilience Architecture
 - Data Protection (BC/DR, Snapshots, etc.)
 - Name Node Continuous Availability
 - SEC 17a-4 Compliant WORM



EMC²

Pivotal

RSA

vmware[®]



TRUSTED BIG DATA

PRIVACY

KNOWLEDGE

EASY

ROUTINE

MINIMUM JUDGMENT

IDENTIFY

KEEP

EVALUATE

ADAPT



EMC²

Pivotal



vmware[®]





EMC²

Pivotal

RSA[®]

vmware[®]

Thank you!