



NEW SECURITY MODELS

FOR THE INTERNET OF **THINGS**

Davi Ottenheimer
@daviottenheimer
New York, June 2014

EMC²



Agenda

- Background
- Security Models at Scale
- Security of Things



Background

Billions and Billions of
Things Connecting
(with each other)
in the Coming Years

Let's Talk About This





Without Forgetting This

If every snowflake a thing...

Without Forgetting This



Reach

Public

Commerce

Military

RFID tags
destroyed in
Somalia

Livestock
tags missing

Mobile crypto
tools

1992

2002

2012



スマートフォンリモコン※1,2

Bluetooth®※3 無線技術でお持ちのスマートフォンからリモコン操作。
トイレ本体と同期して今までのリモコンでは実現できなかった機能を搭載。



リモコン機能

シャワートイレの個人設定や、スマートフォンに保存している音楽をトイレ本体のスピーカーで再生できます。

トイレ日記

日々の排便状況をカレンダー上に記録して、健康管理に活用いただけます。

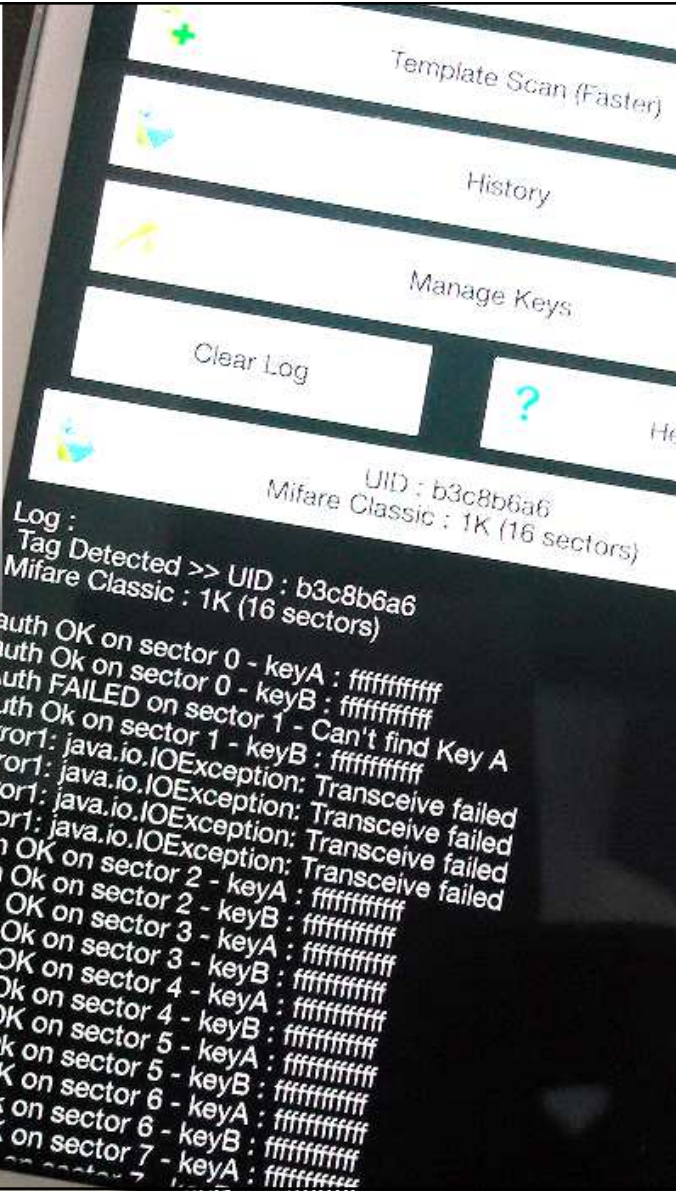
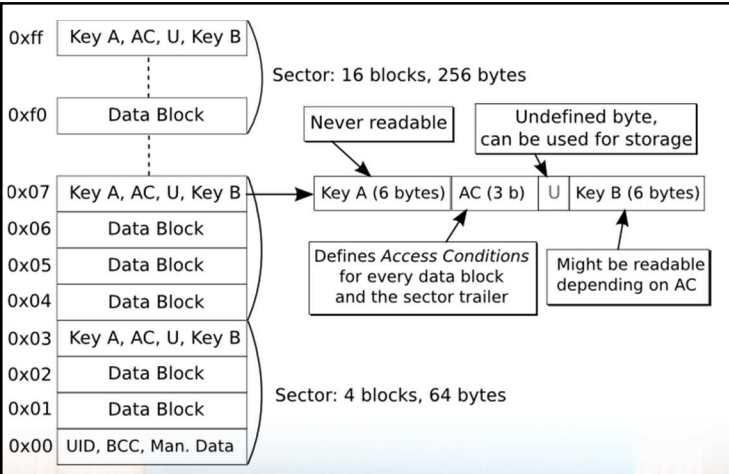
- ※1 スマートフォンリモコンはアンドロイドのみに対応します。
- ※2 市販アプリ「My SATIS」のサービス内容、画面デザインは予告なく変更する場合があります。
- ※3 Bluetooth®は、米国Bluetooth SIG, Inc. の登録商標です。



Bluetooth



“Welcome to
Your Hotel...”



Sector 2:
 00000000000000000000000000000000
 00000000000000000000000000000000
 00000000000000000000000000000000
 ffffffffffffffff078069ffffffffffff

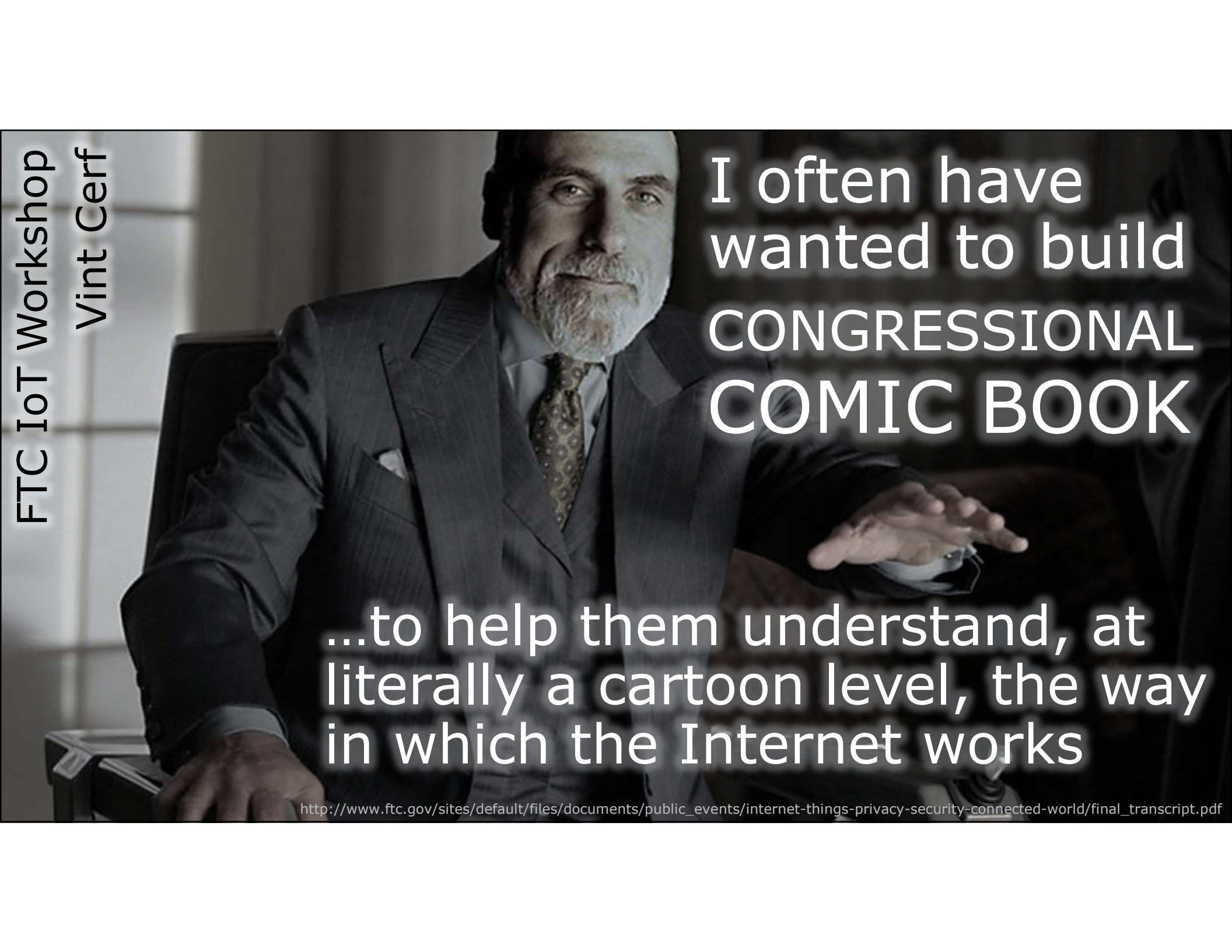
Sector 3:
 00000000000000000000000000000000
 00000000000000000000000000000000
 00000000000000000000000000000000
 ffffffffffffffff078069ffffffffffff

Sector 4:
 00000000000000000000000000000000
 00000000000000000000000000000000
 00000000000000000000000000000000
 ffffffffffffffff078069ffffffffffff

Sector 5:
 00000000000000000000000000000000
 00000000000000000000000000000000
 00000000000000000000000000000000
 ffffffffffffffff078069ffffffffffff

Sector 6:
 00000000000000000000000000000000
 00000000000000000000000000000000
 00000000000000000000000000000000
 ffffffffffffffff078069ffffffffffff

Sector 7:
 00000000000000000000000000000000
 00000000000000000000000000000000
 00000000000000000000000000000000

A photograph of Vint Cerf, a man with a grey beard and mustache, wearing a dark suit, white shirt, and patterned tie. He is sitting in an office chair, looking towards the camera with a slight smile. His right hand is resting on a desk, and his left hand is raised in a gesture. The background is a blurred office setting with a window.

I often have
wanted to build
CONGRESSIONAL
COMIC BOOK

...to help them understand, at
literally a cartoon level, the way
in which the Internet works

FTC IoT Workshop 2013

1. What are the significant developments in services and products that make use of this connectivity (including prevalence and predictions)?
2. What are the various technologies that enable this connectivity (e.g. RFID, barcodes, wired and wireless connections)?
3. What types of companies make up the smart ecosystem?
4. What are the current and future uses of smart technology?
5. How can consumers benefit from the technology?



Definition and Benefits

6. What are the unique privacy and security concerns associated with smart technology and its data? For example, how can companies implement security patching for smart devices?
7. What steps can be taken to prevent smart devices from becoming targets of or vectors for malware or adware?
8. How should privacy risks be weighed against potential societal benefits, such as the ability to generate better data to improve health-care decision-making or to promote energy efficiency?
9. Can and should de-identified data from smart devices be used for these purposes, and if so, under what circumstances?

FTC IoT Workshop 2013

- 6. Unique** privacy and security concerns (patching)
- 7. Non-unique** concerns (prevent becoming malware or adware targets or vectors)
- 8. Privacy** risk benefit balance
- 9. De-identified data** ok to be used, and when?

Security

FTC IoT Workshop 2013

Challenges

Consumer Data Collection
Unexpected Uses
Data Protection

VS

Best Practices

Privacy by Design
Simplified Choice
Transparency

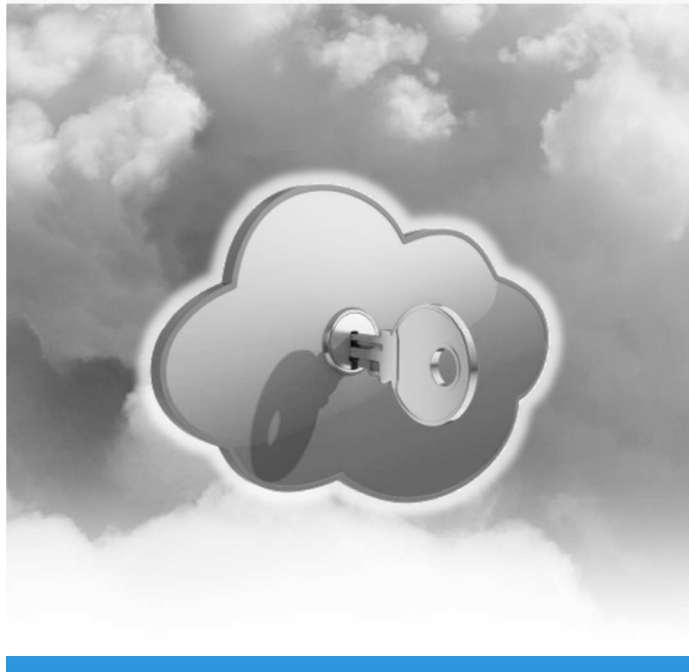
Privacy

Visibility

Resilience

EMC²

Privacy



Visibility



Resilience





Security Models at Scale

1. Resilience



1996 Ariane 5 Lesson

One-Chance to Get it Right

“software should be **assumed to be faulty**”

“concern software exception is allowed, or even required, to cause processor halt on mission-critical equipment”

1998 Update Distribution Problem

- 10,000+ Systems
- Critical Infrastructure
- Ping Discovery = Abend (Operations Shutdown)



2002 Update Distribution Problem

- 140,000 Distributed U.S. Critical Systems
- 80% "Report" Patch Success (28,000 Unpatched)
- Varied Patch Integrity



2005 Update Distribution Problem

- 2 Billion Users
- 100s Millions Distributed Systems
- Go/No-Go Launch Decisions
- “One-Chance to Get it Right”???



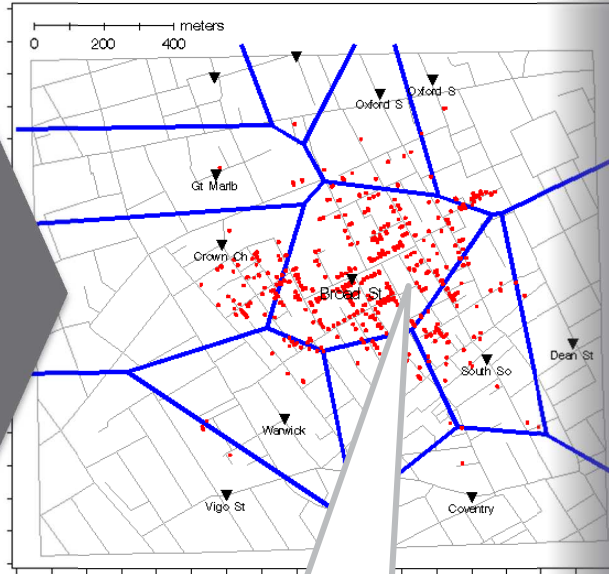
2012 RSAC: Snow Den Lesson

1854: GHOST MAP

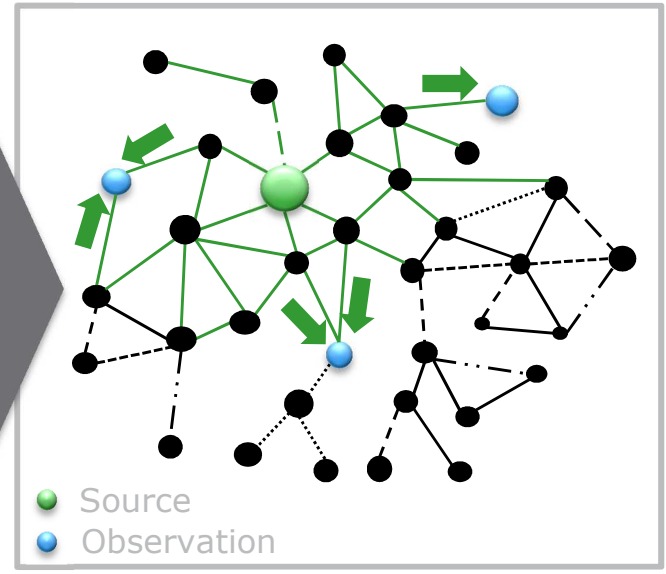


Dr. John Snow
1813-1858

1854: CHOLERA VORONOI



NETWORK BREACH DATA



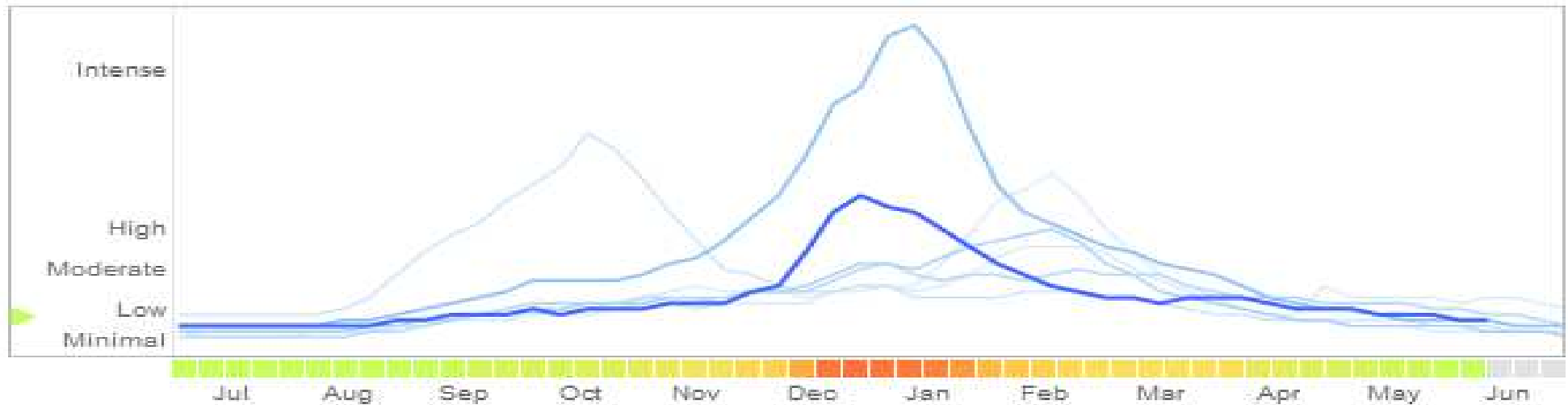
<http://www.flyingpenguin.com/?p=18259>



Google Wrong 3rd Year in a Row

"Algorithmic accountability is one of the biggest problems of our time"

"...system consistently overestimated flu-related visits over the past 3 years, and was especially inaccurate around the peak of flu season – when such data is most useful."



<http://www.google.org/flutrends/us/>

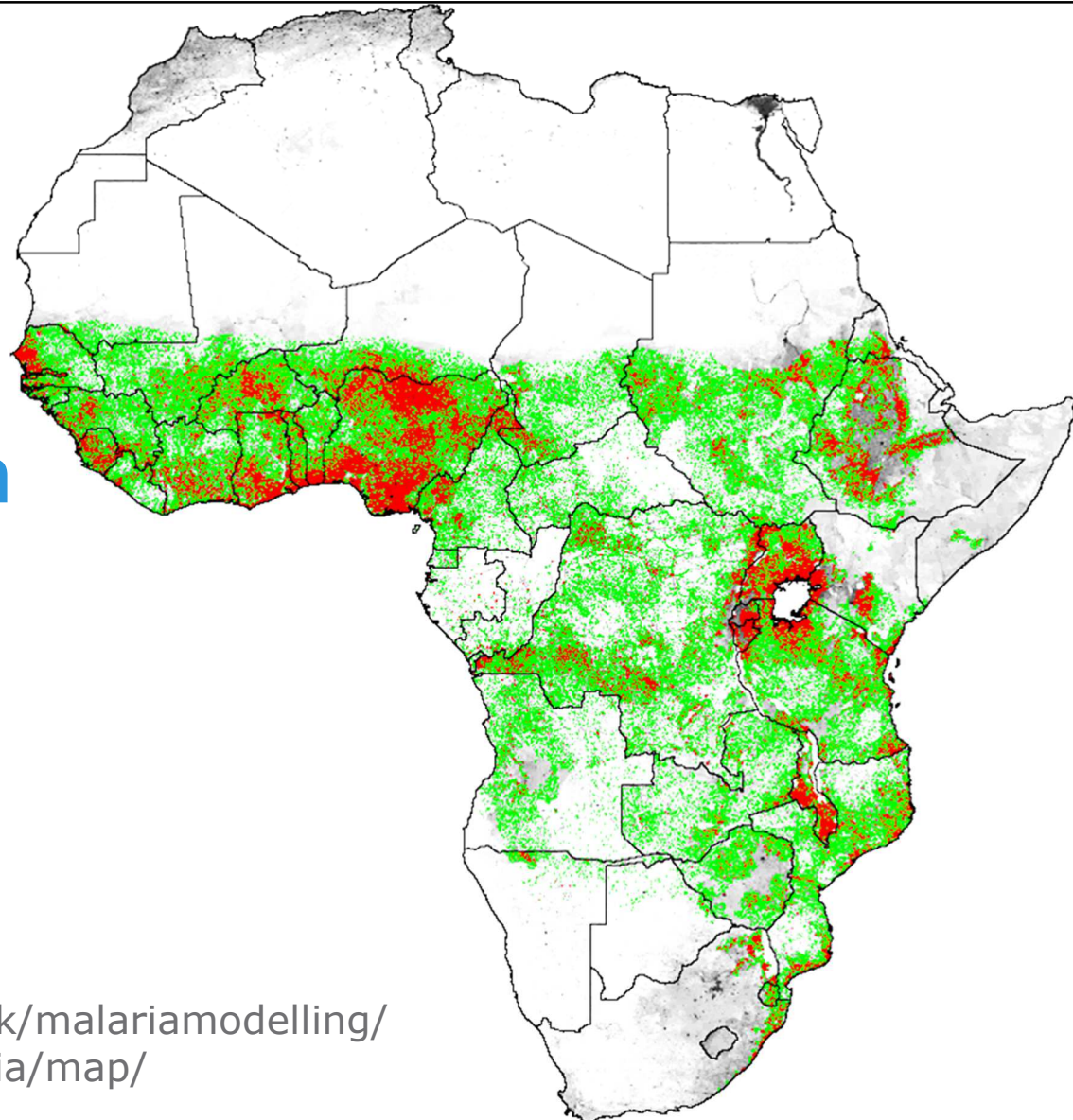
<http://www.newscientist.com/article/dn25217-google-flu-trends-gets-it-wrong-three-years-running.html>

© Copyright 2014 EMC Corporation. All rights reserved.

EMC²

Vaccines "Solving" Malaria...

(Supply-Chain
Risk Factor)



<http://www1.imperial.ac.uk/malariamodeling/>
<http://www.cdc.gov/malaria/map/>

+ Add to Directory Export Data

Patching "Solving" Windows XP

Services

HTTP	1,329,548
RDP	874,912
MySQL	548,328
SMTP	222,093
FTP	148,368

Top Countries

United States	2,297,837
China	162,097
Germany	98,615
United Kingdom	80,109
Russian Federation	70,248

Windows XP
 China Unicom Shandong
 Added on 24.05.2014
 Jinan
[Details](#)

HTTP/1.0 403 Forbidden
 Content-Type: text/html; charset=gbk
 Content-Length: 106
 Connection: close

Windows XP
 China Telecom Chongqing
 Added on 24.05.2014
 Chongqing
[Details](#)

HTTP/1.0 403 Forbidden
 Content-Type: text/html; charset=gbk
 Content-Length: 106
 Connection: close



Computers Are Not A Pet



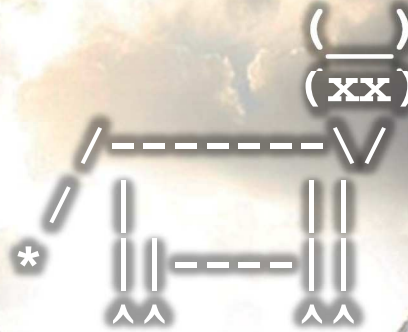
Are They Cows?



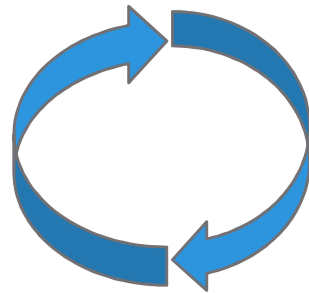
Or Cows...



Resilience = Systematic Treatment



Easily Identified
Routine Treatment
Minimum Judgment

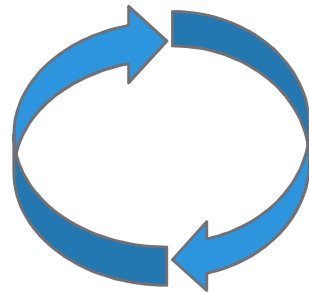


Identify Sick ASAP
Keep Adequate Records
Evaluate Daily Sick
Adapt Until Improvement Noted

Resilience = Intelligence Driven

PATCH

Easily Identified
Routine Treatment
Minimum Judgment



ANALYZE

Identify Sick ASAP
Keep Adequate Records
Evaluate Daily Sick
Adapt Until Improvement Noted

2. **Visibility**

(Simplified Choice)



DON'T GO

GO

Regulatory Compliance: A Little Light Humor



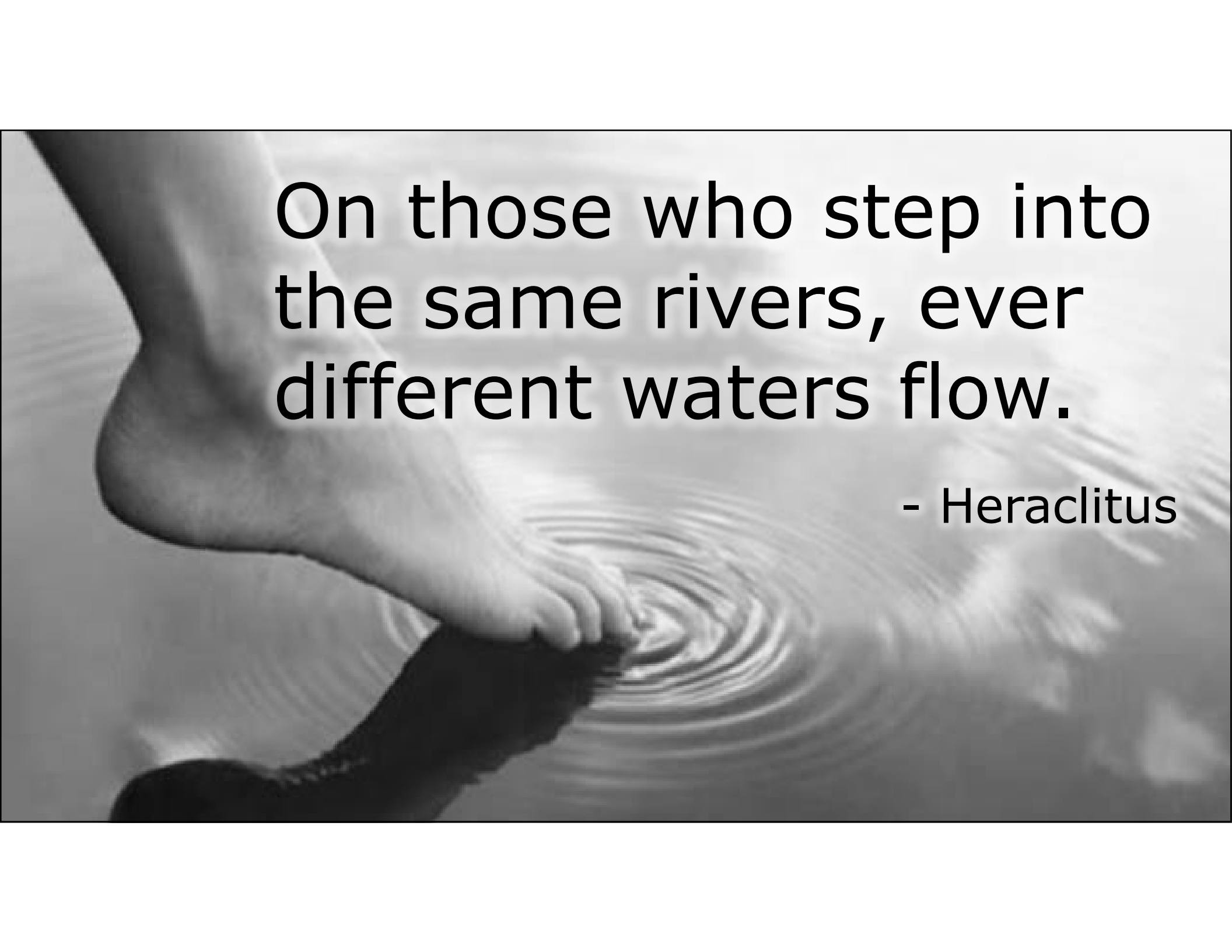
GO

DON'T GO





Everything
Always is Different

A black and white photograph showing a person's foot stepping into water. The foot is in the lower-left foreground, and the water surface is filled with concentric ripples that spread outwards. The background is a soft, out-of-focus view of water. The overall mood is contemplative and philosophical.

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

- Heraclitus

We've Been
Here Before



The longer you can
look back, the
farther you can
look forward.

- Winston Churchill

Churchill by Himself (2008), Appendix I: Red Herrings, ed. Langworth, Public Affairs, p. 577

EMC²

Induction Fallacy and Probability Models

Knowledge for Actionable Insights to Inform Priorities



The wise
proportion
belief to
evidence.

Simplified Choice = Know *Everything*?



3. Privacy

No Reasonable Expectation of Privacy



- In speed on a public highway
- In use of a vehicle's brakes

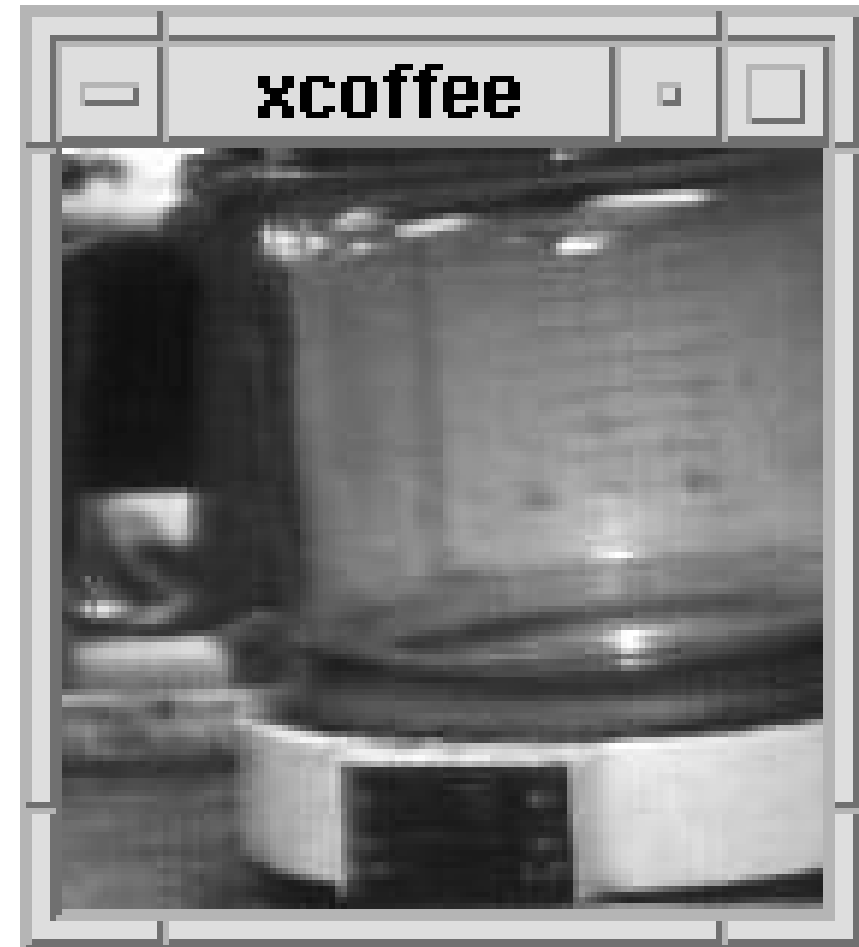
...because statutorily required brake lights announce use to the public....

...technology merely captured information defendant knowingly exposed to the public

<http://www.courts.ca.gov/opinions/documents/A137796.DOC>

Do You Want...Coffee?

- Update 3x/min
...because pot filled slowly
- Greyscale
...because so was the coffee



<http://www.cl.cam.ac.uk/coffee/coffee.html>

3. *“Knowledge”*

The *Relative* Acceptability of Knowledge

Microsoft Technology Policy Group, Trust Survey 2012-2013

Personalized Experience

Canada

Sweden

U.S.A.

Germany

U.K.

Australia

VS

Community Benefit

China

India

(jumps from 5% to 12%)

http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf

© Copyright 2014 EMC Corporation. All rights reserved.

EMC²

Anyone Want This?



Or This?

42



Or This?



Top-Down Things Scary



“They’re Everywhere!”

Israeli Thing Exports

1. Rock Listening Devices in Lebanon
2. Sharks Mossad-trained in Egypt
3. Vulture Mossad-trained in Saudi Arabia, Sudan

“bird found in rural area of country wearing transmitter and leg bracelet bearing the words ‘Tel Aviv University’”

Open Peers Hot

"Smart Dust"



What They Want to Know

**Personalized
Experience**

**Community
Benefit**

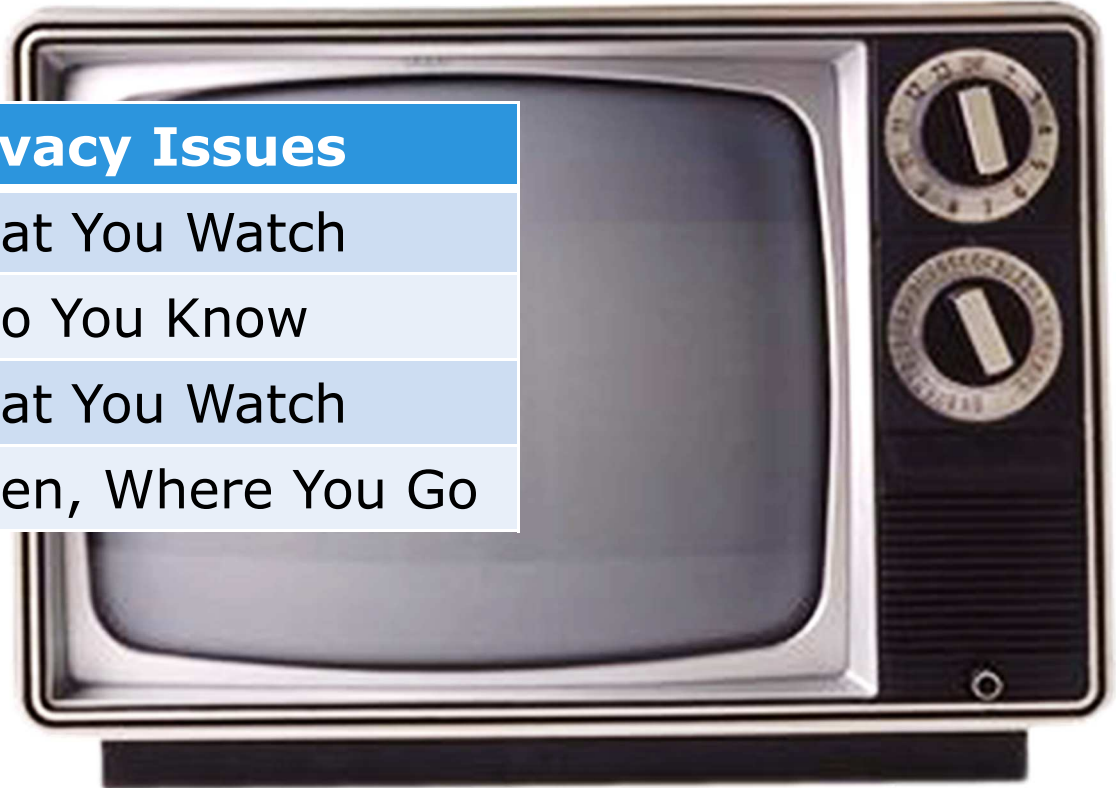
What You Want Known

EMC²

TVs as Things

Surveillance of the Home

Offered	Privacy Issues
Reduced Advertisements	What You Watch
Sharing	Who You Know
Targeting	What You Watch
Anywhere Availability	When, Where You Go



Cars as Things

Surveillance of the Road: Sensors on Wheels

Offered	Privacy Issues
Reduced Response Time	Where You Drive
Reduced Insurance Rate	Where and How You Drive
Reduced Taxes	Where You Drive
Sharing	Who You Know
Congestion Avoidance	Everyone Else's Data
Driver-less	Everything

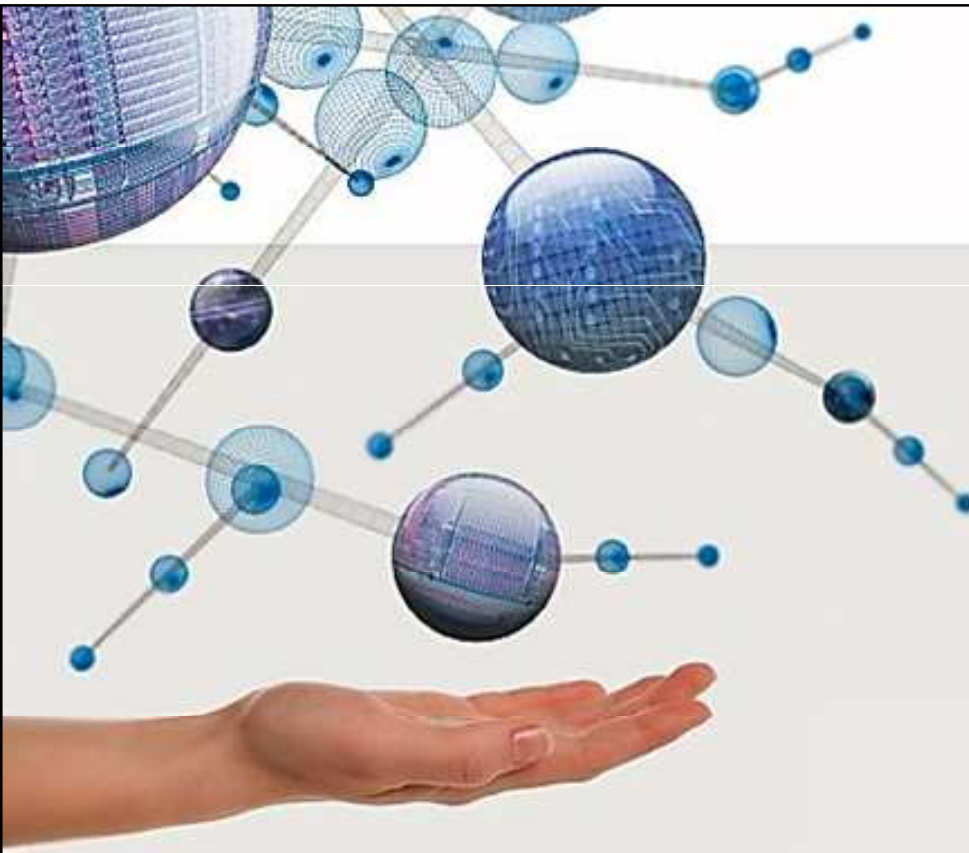
“an exoskeleton that gives you superhuman powers”
- Scott Lange



EMC²



Security of Things



- FIPS 140-2 Level 3
- Dual eSi-3250 Proc
- 1MB Embed Flash
- USB, I2C, UART, NFC...

© Copyright 2014 EMC Corporation. All rights reserved.

- Encryption Acceleration
- Active Shield Protection
- Mesh Sensor
- Detection
 - Voltage
 - Temperature
 - Clock
 - Physical tamper
- Key Memory Battery Backup
- Auto Erase
- EMV L1/L2 Firmware Contact and Contactless

EMC²

What They Want to Know
Identify, **K**eep, **E**valuate, **A**dapt

**Personalized
Experience**

**Community
Benefit**

What You Want Known
Easy, **R**outine, **M**inimal Judgment

Example: SCADA

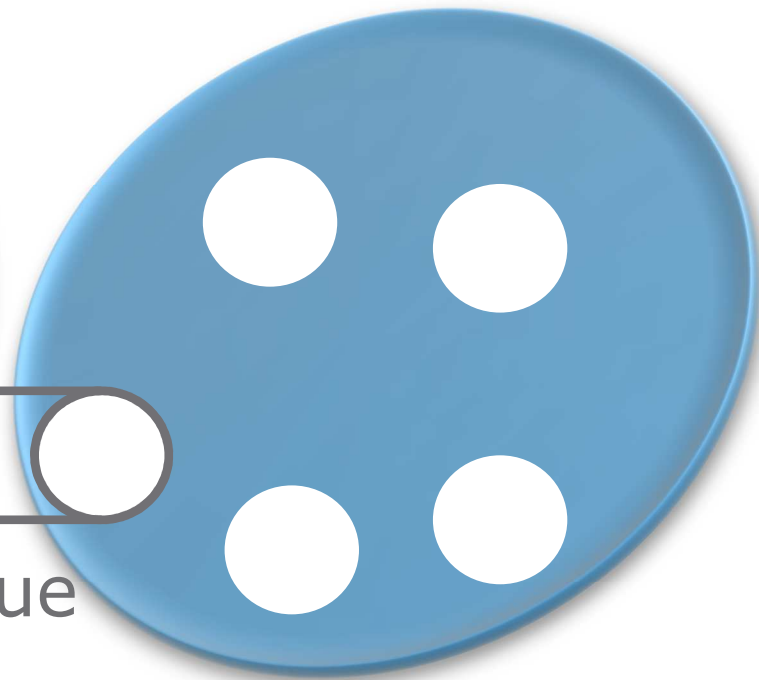
Semantic Security Monitoring of Industrial Control Systems

- 20-40 Year Lifetime
- Can Not Be Upgraded
- Not Built With Security
- Simple, Predictable / Routine Operations





Thing
Platform

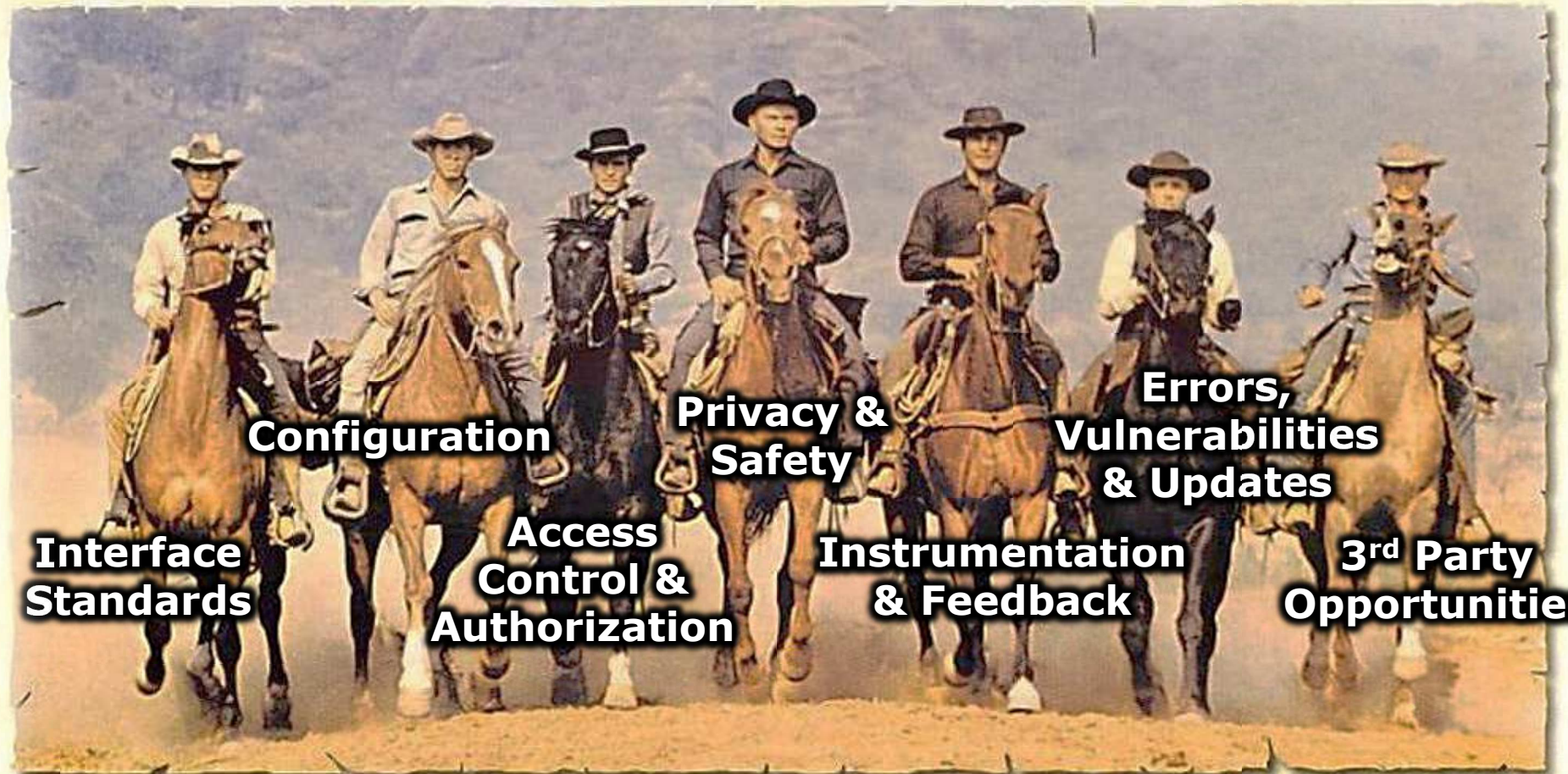


Human
Platform



MAGNIFICENT SEVEN

They fought like seven hundred



**Interface
Standards**

Configuration

**Access
Control &
Authorization**

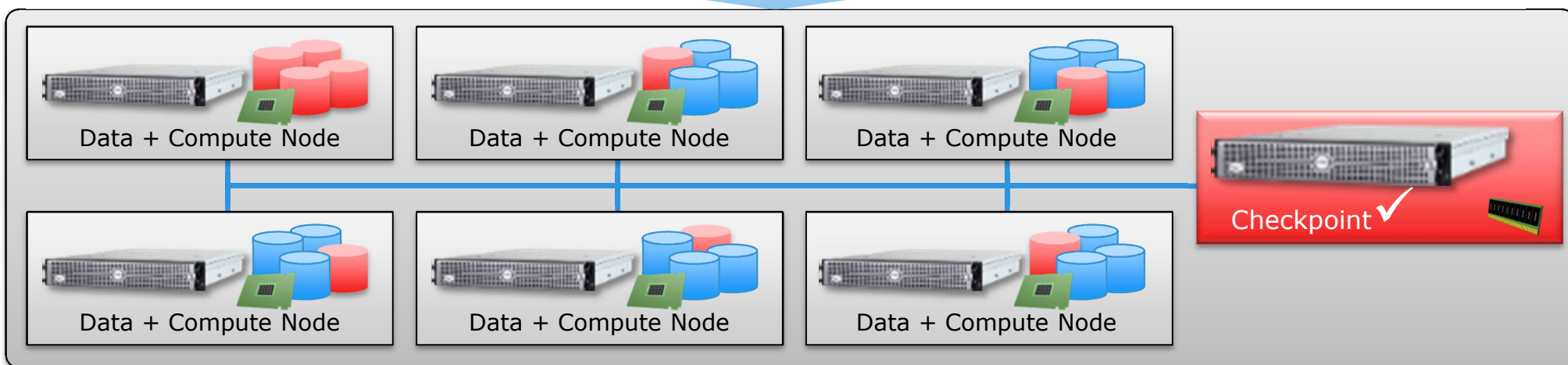
**Privacy &
Safety**

**Instrumentation
& Feedback**

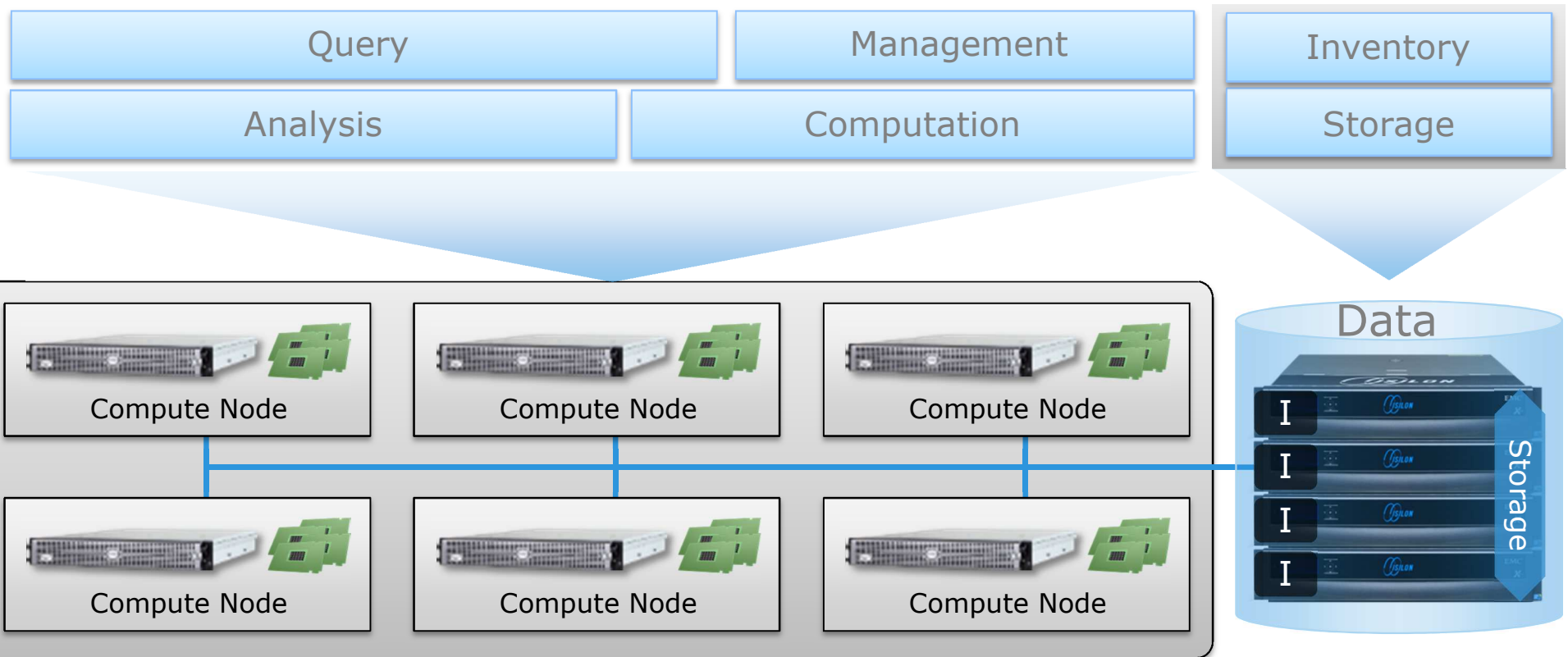
**Errors,
Vulnerabilities
& Updates**

**3rd Party
Opportunities**

Phase One - Connectivity

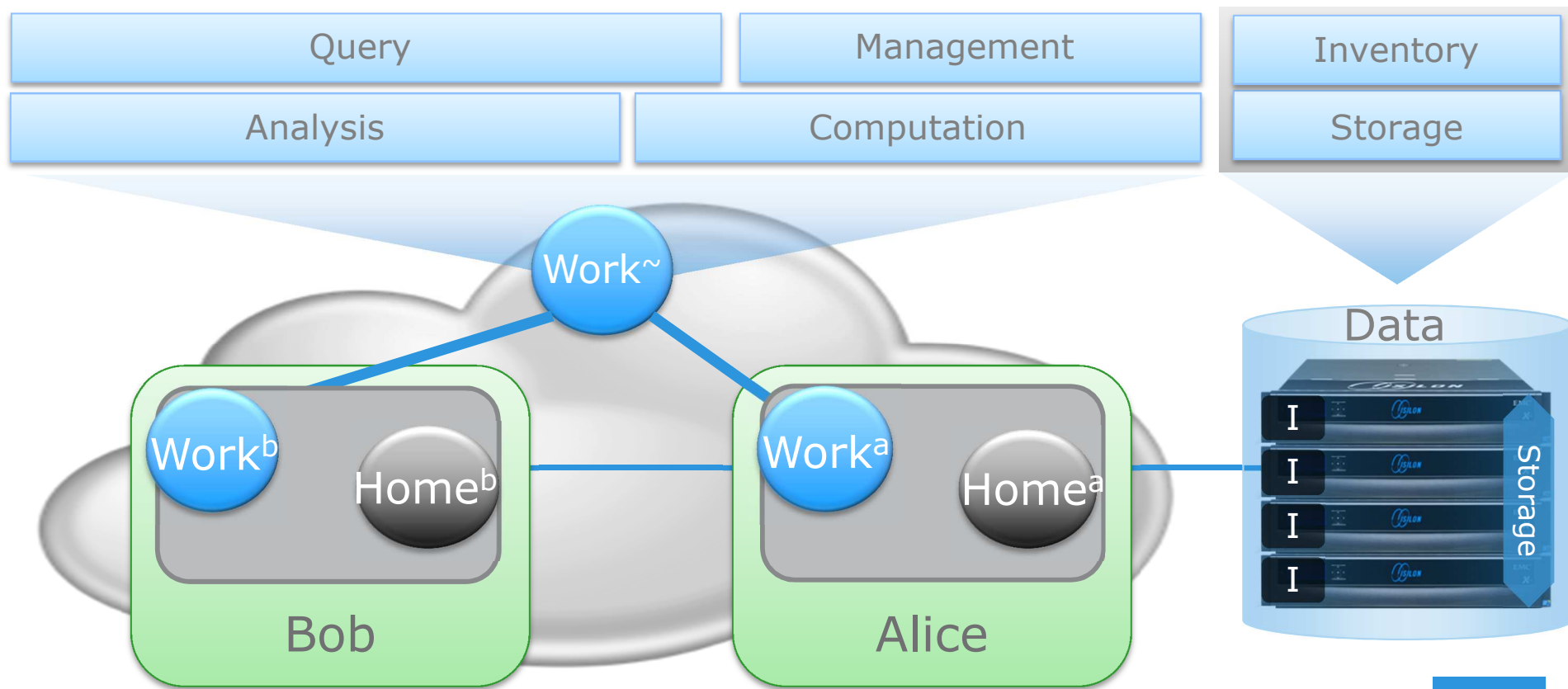


Phase Two - Resilience

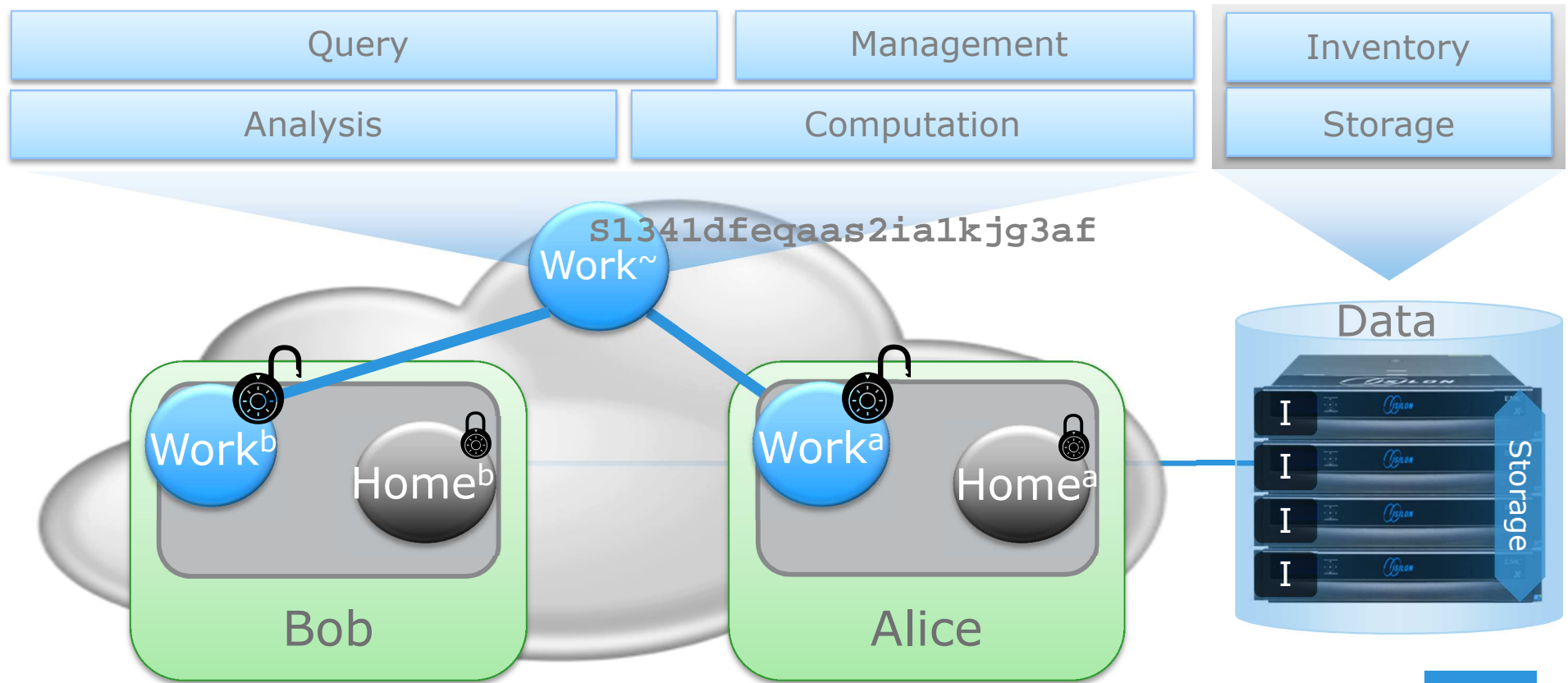


EMC²

Phase Three - Classification



Phase Four – Least Authority



EMC²

Phase Five – Connectivity...(Repeat)

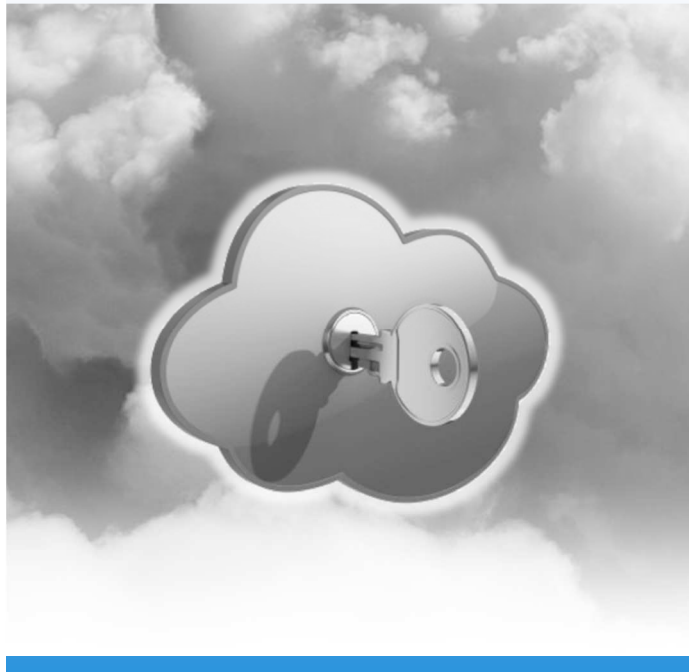


IoT Requires New Relationships



New Relationships Require Trust

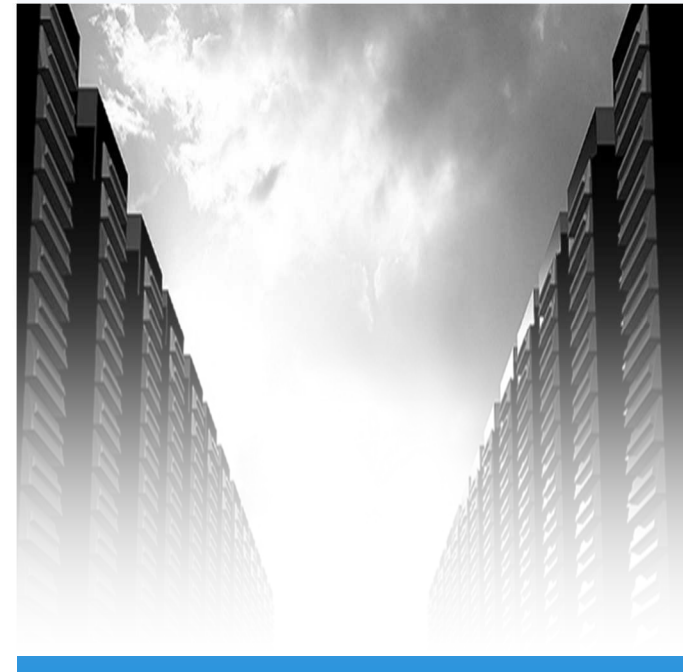
Privacy



Visibility



Resilience





Thank You!

NEW SECURITY MODELS

FOR THE INTERNET
OF **THINGS**

Davi Ottenheimer
Senior Director of Trust
[@daviottenheimer](#)



EMC²



EMC²

Pivotal

RSA[®]

vmware[®]