Into the Cloud with SCAP

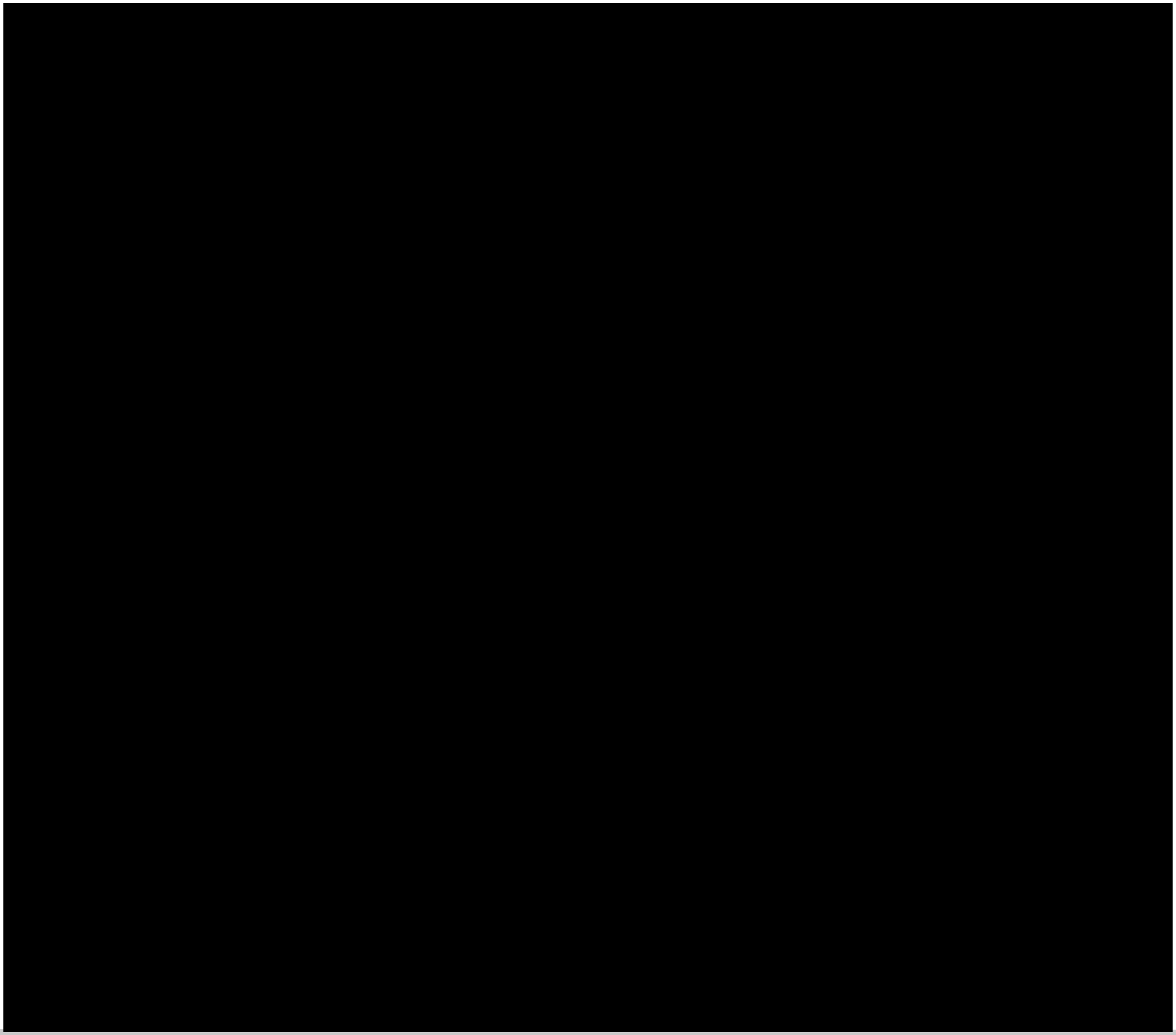
Digital Trust in the Cloud

Liquid Security in Cloudy Places

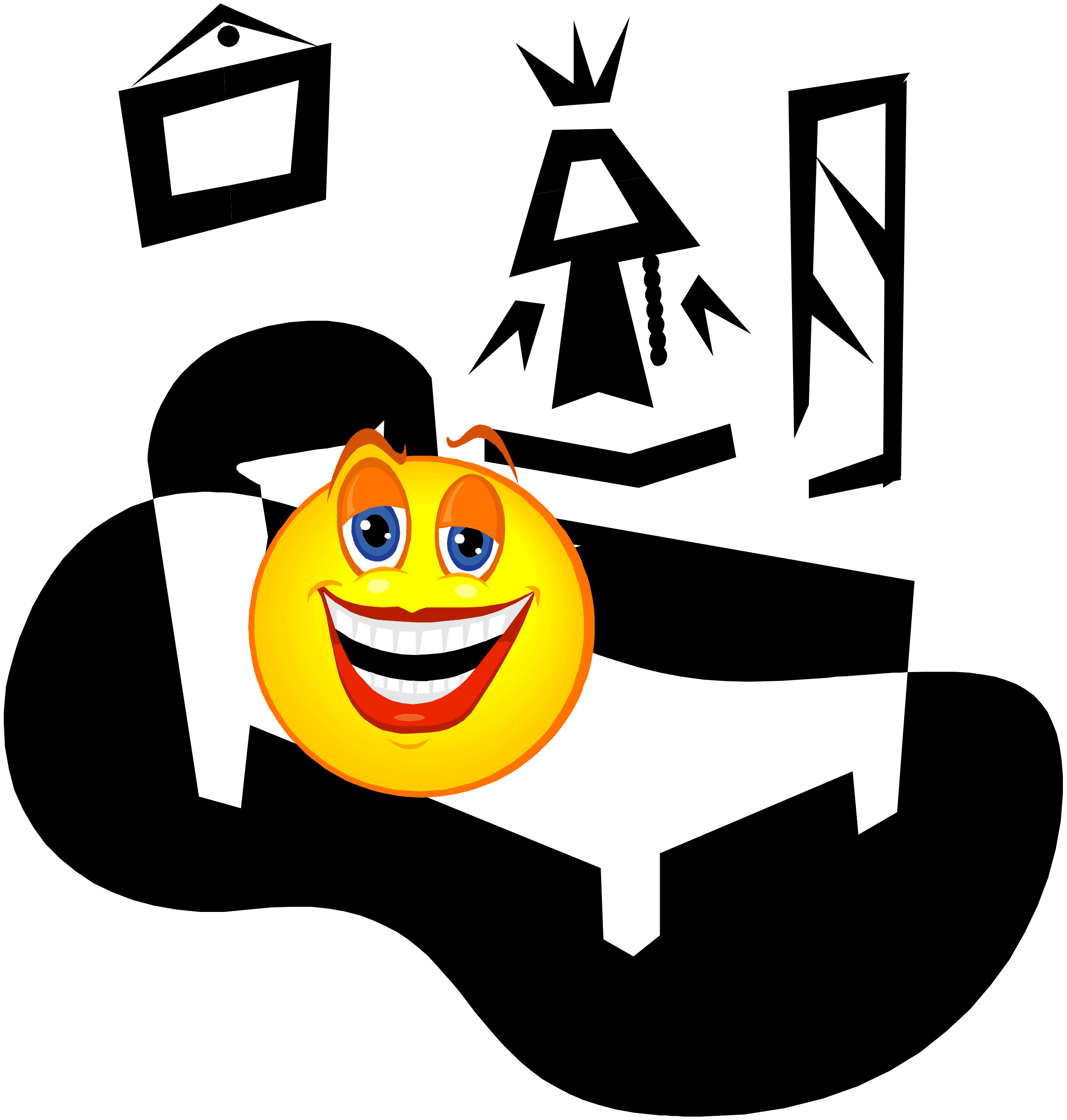
Ron Knode

October 2009

Are You Afraid of the Dark?

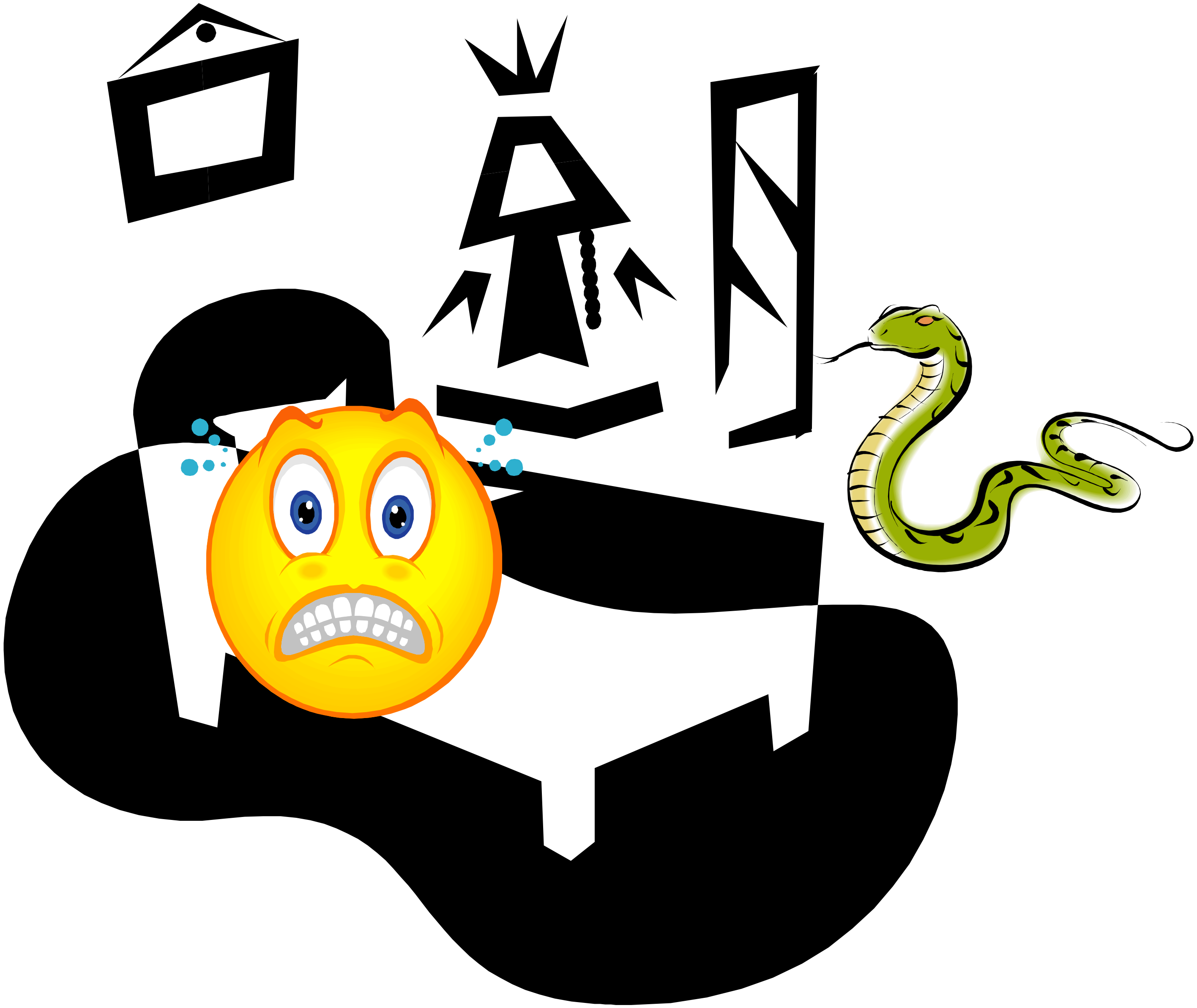


Are You Afraid of the Dark?



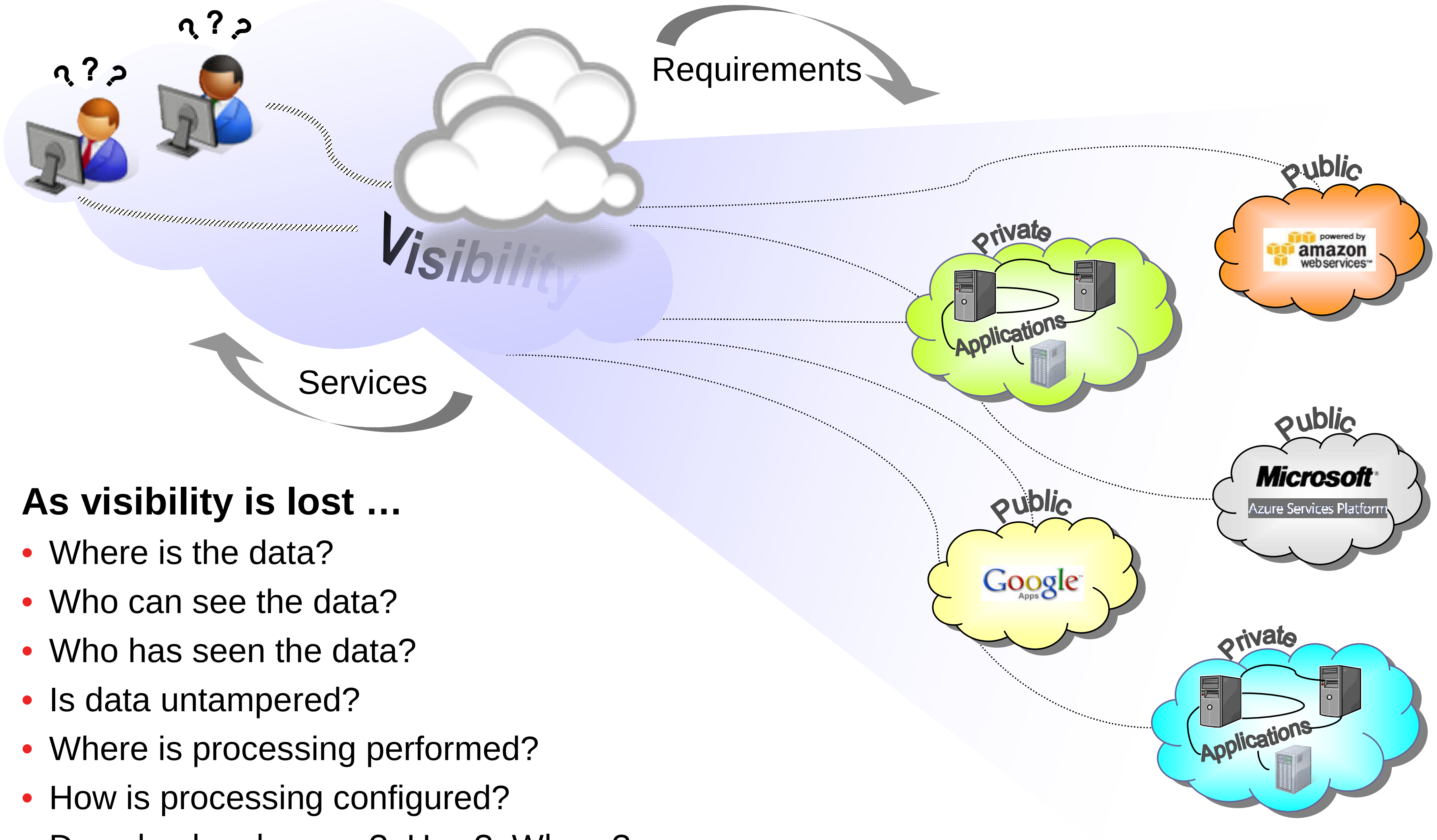
Are You Afraid of the Dark?

Are You Afraid of the Dark?



Information Assurance is Cloud-Complicated

“Clouds are cloudy”



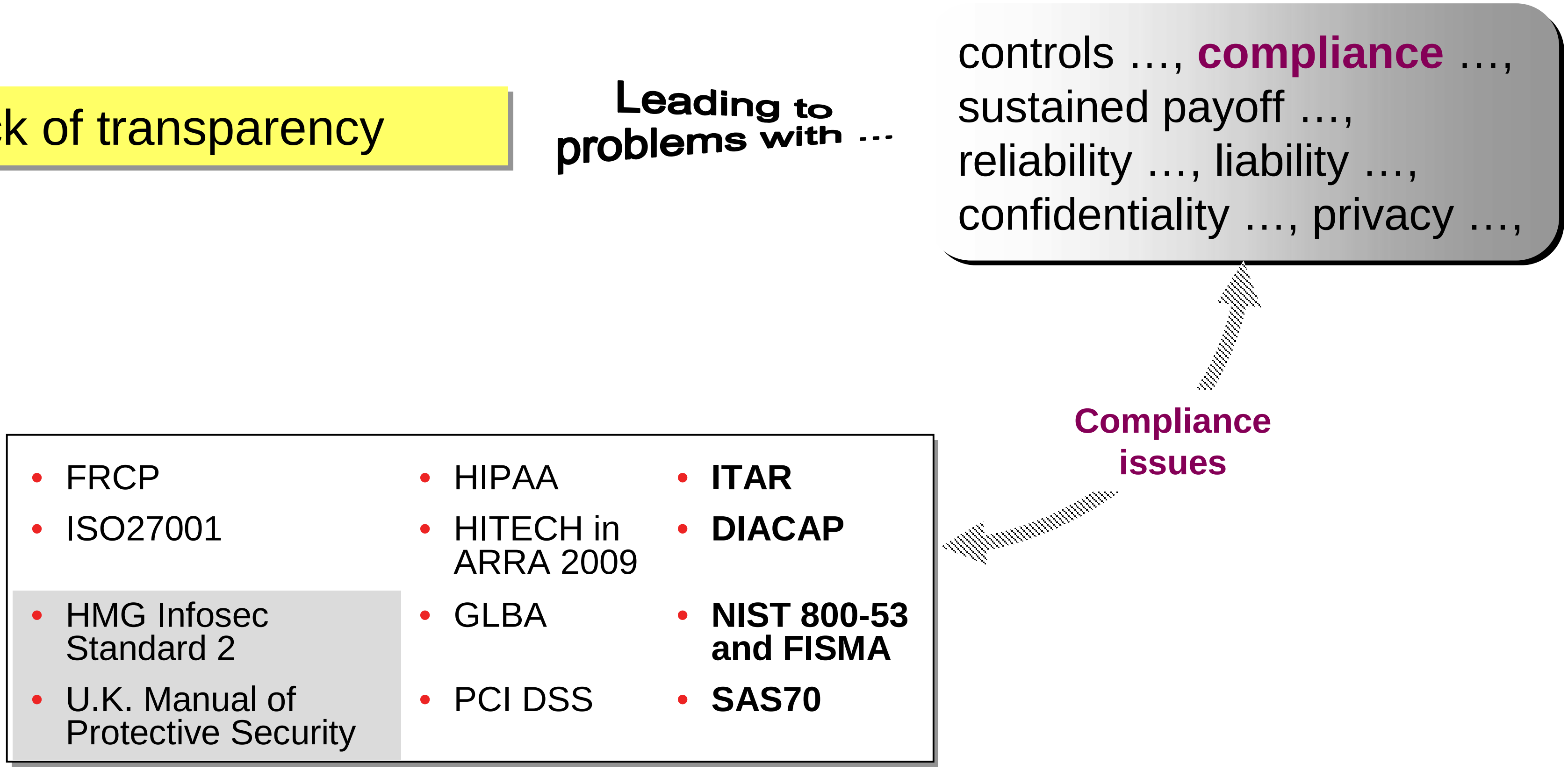
As visibility is lost …

- Where is the data?
- Who can see the data?
- Who has seen the data?
- Is data untampered?
- Where is processing performed?
- How is processing configured?
- Does backup happen? How? Where?

… Security, compliance, and value are lost as well

Cloud Processing
Three Big Obstacles to Value Capture

- Lack of standards
- Lack of portability
- Lack of transparency



Leading to problems with …

controls …, **compliance** …, sustained payoff …, reliability …, liability …, confidentiality …, privacy …,

Compliance issues

- FRCP
- ISO27001
- HMG Infosec Standard 2
- U.K. Manual of Protective Security
- HIPAA
- HITECH in ARRA 2009
- GLBA
- PCI DSS
- **ITAR**
- **DIACAP**
- **NIST 800-53 and FISMA**
- **SAS70**

Absent Transparency … Some Big Problems

For example, … without transparency …

- No confirmed chain of custody for information
- No way to conduct investigative forensics
- Little confidence in the ability to detect attempts or occurrences of illegal disclosure
- Little capability to discover or enforce configurations
- No ability to monitor operational access or service management actions (e.g., change management, patch management, vulnerability management, …)

Weatherproofing the Enterprise for Cloud Services Today

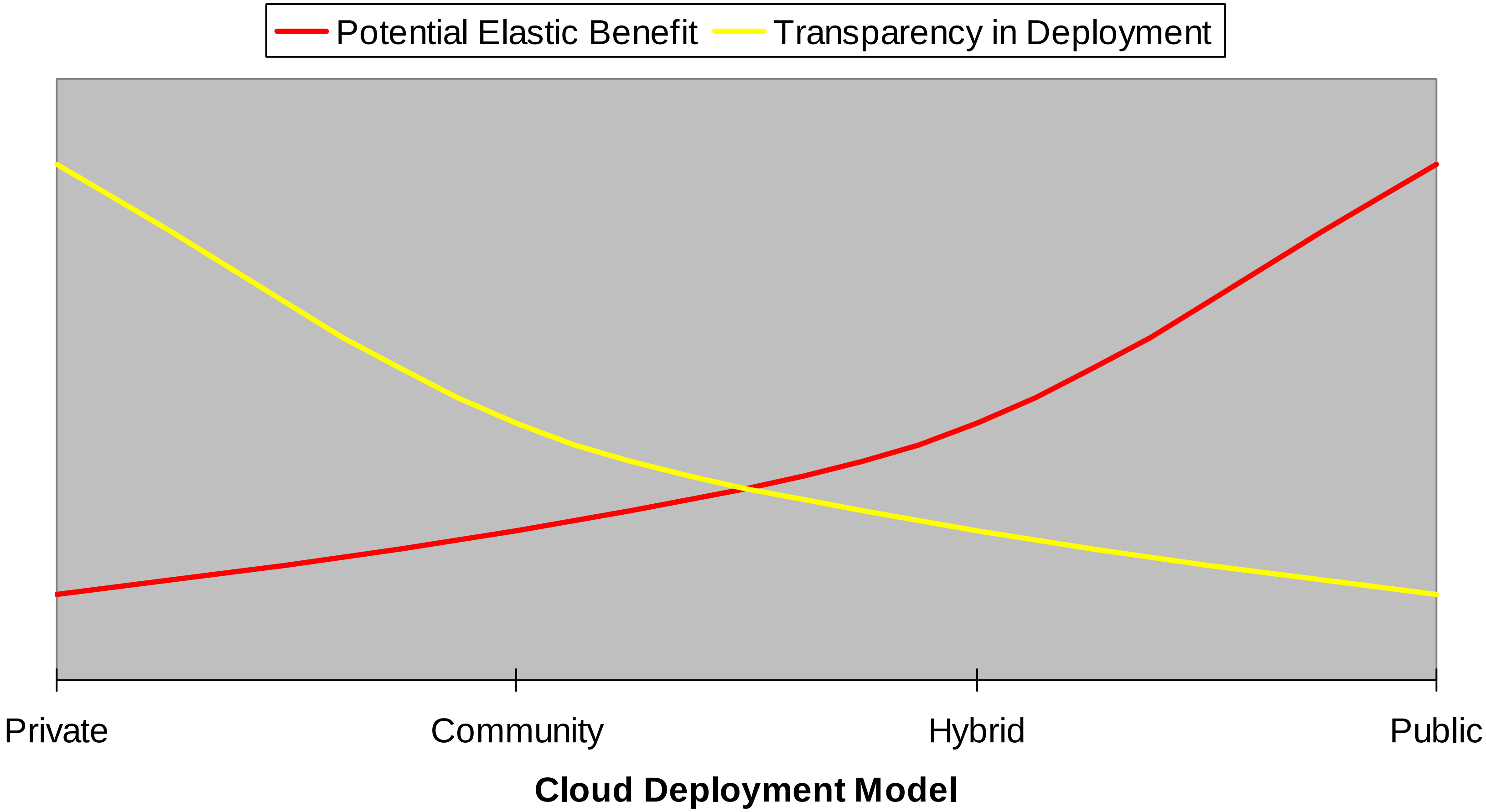
Waiting for liquid security to evolve

Private Clouds

“Safe Computing” for Cloud Processing

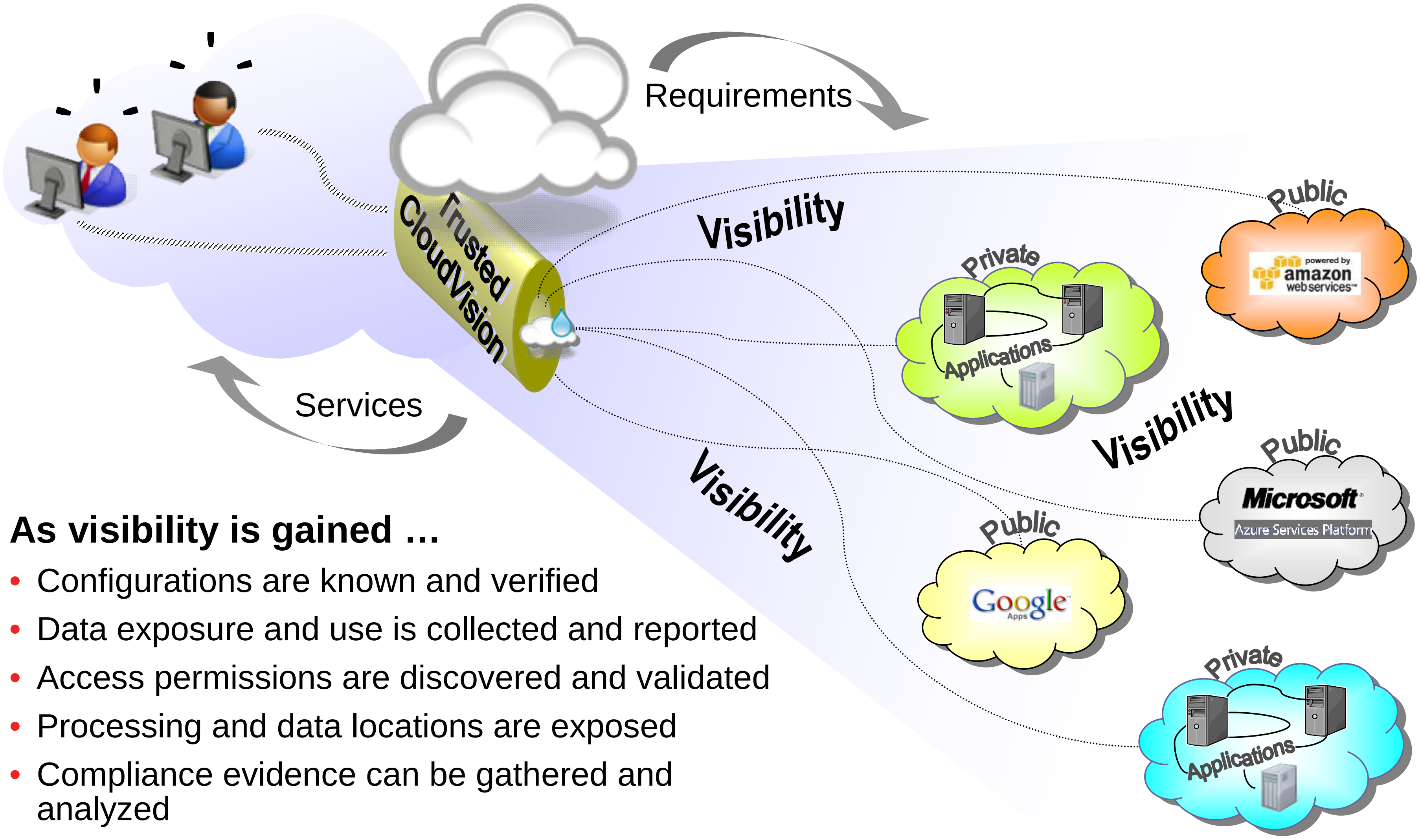
Presumptive Security

Relationship between Transparency and Elastic Payoff Potential based on Deployment Model



Transparency Restores Information Assurance

Working with a “glass cloud” delivers the elastic benefits of the cloud



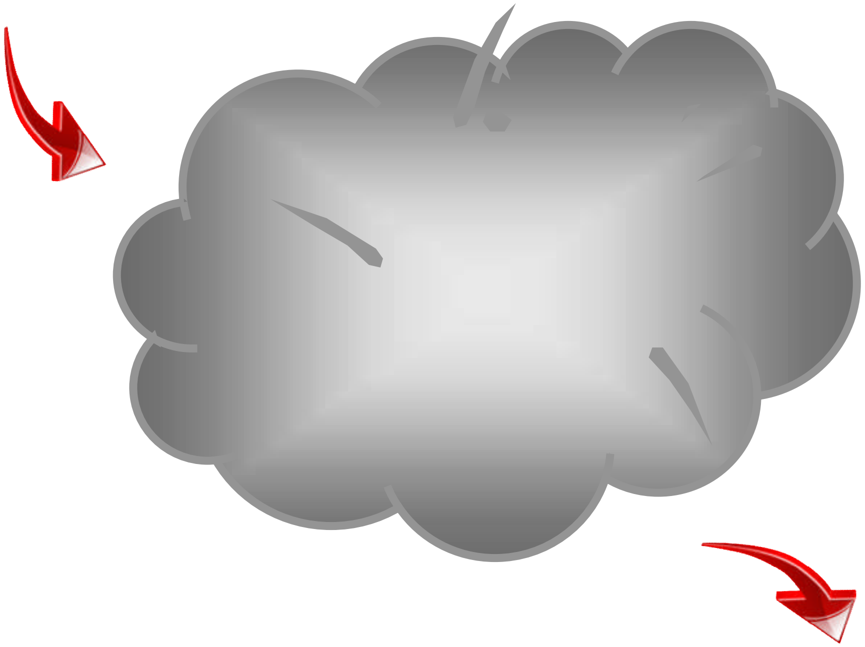
As visibility is gained …

- Configurations are known and verified
- Data exposure and use is collected and reported
- Access permissions are discovered and validated
- Processing and data locations are exposed
- Compliance evidence can be gathered and analyzed
- Processing risks and readiness become known

… Security, compliance, and value are captured as well

The Real Value Question for Cloud Processing

- **How do we create digital trust in the cloud so we can reap the greatest elastic benefit?**

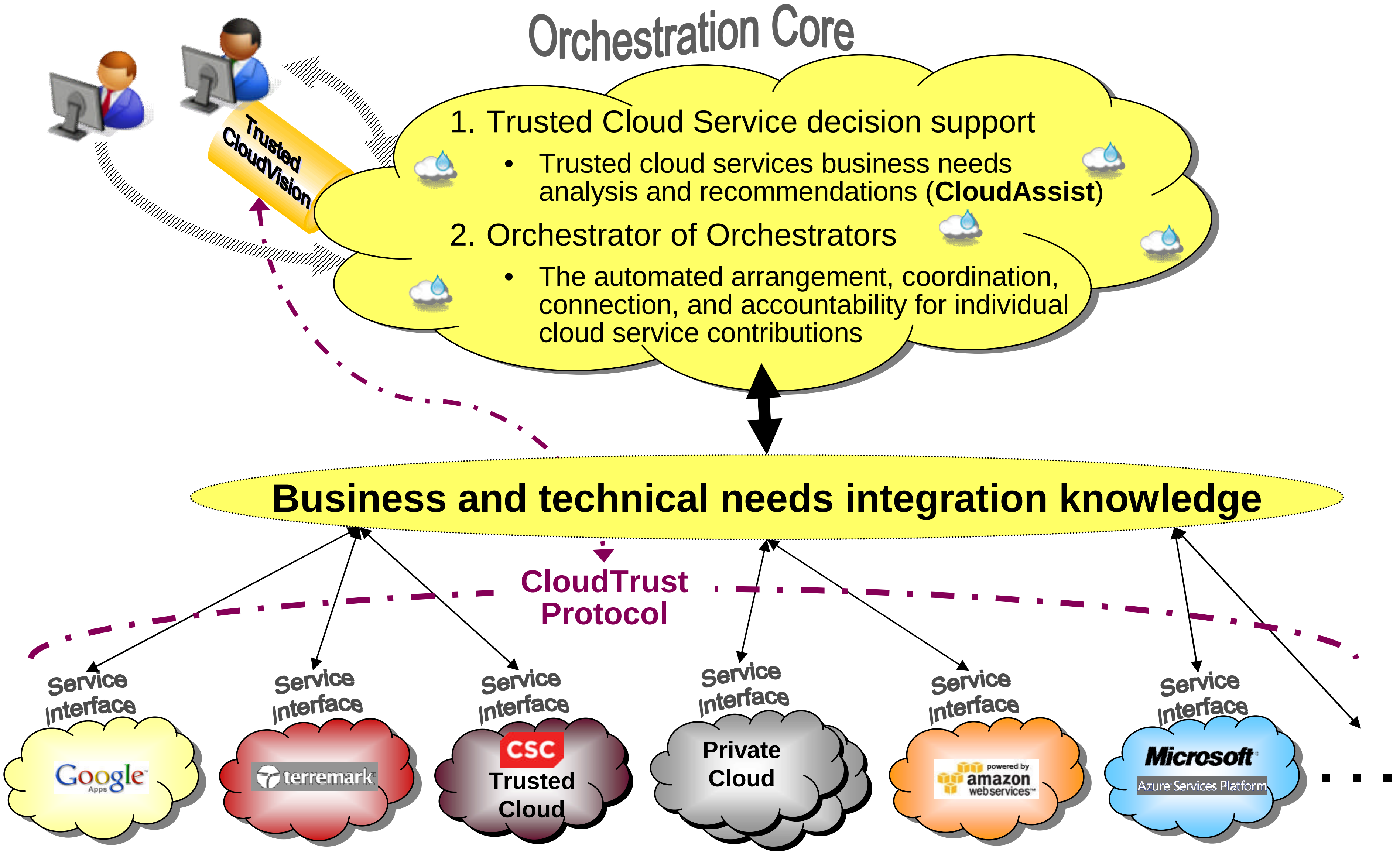


Without disqualifying any cloud provider or consumer … ?!

- **How do we bring transparency to the cloud so we can reap the greatest elastic benefit?**

The Orchestration Core

Translation of Business Needs to Trusted Cloud Service Delivery



1. Trusted Cloud Service decision support
   - Trusted cloud services business needs analysis and recommendations (**CloudAssist**)
2. Orchestrator of Orchestrators
   - The automated arrangement, coordination, connection, and accountability for individual cloud service contributions

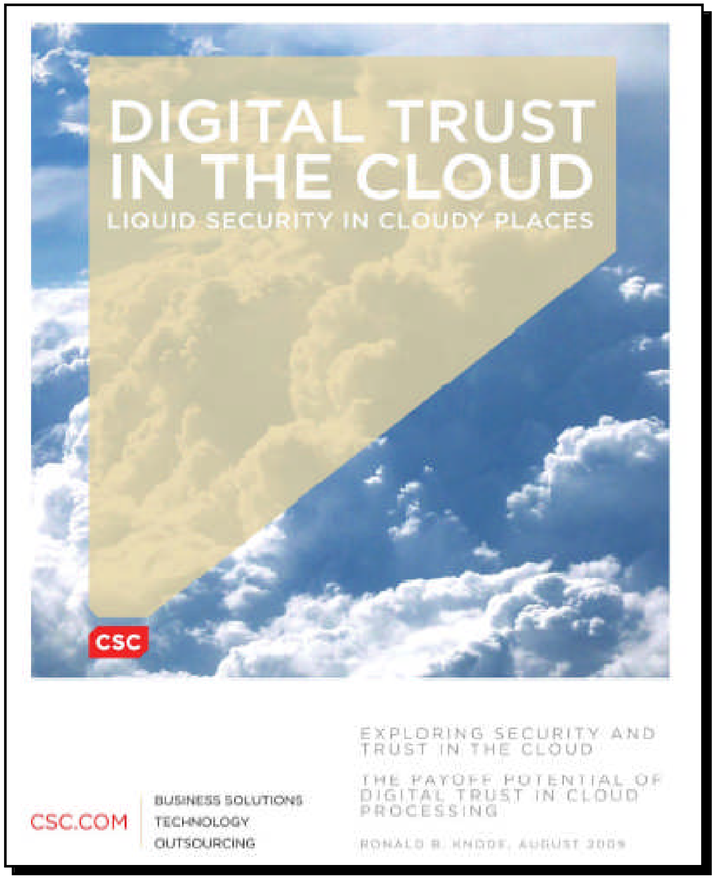
Trusted CloudVision™
CloudTrust Protocol (CTP) Activation **Sample**

CloudTrust™ Protocol Representation

Type	Family	Information Request or Delivery
Initiation	**Identity / Session**	1. Identify service owner and initiate evidence session 2. Terminate evidence session
Evidence Requests	**Configuration**	[for all cloud service units supporting service owner …]
		3. What is current configuration for {Hypervisor? Guest O/S's? Virtual switches? Virtual firewalls?}
		4. How does current configuration of {service unit type} differ from {service owner configuration specification/policy}
SCAP	**Vulnerability**	[for all cloud service units supporting service owner …]
		5. Results of latest vulnerability assessment on {hypervisor; guest O/S's; virtual switches; virtual firewalls}
		6. Date of latest vulnerability assessment on {hypervisor; guest O/S's; virtual switches; virtual firewalls}
		7. Perform vulnerability assessment now on {hypervisor; guest O/S's; virtual switches; virtual firewalls}
	Anchoring	[for all cloud service units supporting service owner …]
		8. Provide geographic location and affirmation (by unit identity)
		9. Provide platform separation affirmation and identities (by unit identity)
		10. Provide process separation affirmation – positive or negative - (by process name, e.g., storage encryption, storage de-duplication, …)
	Audit Log	[for all cloud service units supporting service owner …]
		11. Provide log of policy violations {in last 'n' hours} (e.g., malware elimination, unauthorized access attempts, …)
		12. Provide audit/event log {for last 'n' hours}
		13. Provide list of currently authorized users/subjects and their permissions
		14. …
Policy introduction	**Users & permissions**	15. … And more …

Research Conclusions Summary

- The desire to benefit from the elastic promise of cloud processing is blocked for most enterprise applications because of security and privacy concerns.
- The re-introduction of transparency into the cloud is the single biggest action needed to create digital trust in a cloud and enable the capture of enterprise-scale payoffs in cloud processing.
- Even today there are ways to benefit from cloud processing while technologies and techniques to deliver digital trust in the cloud are evolving.
- CSC has created a definition and an approach to "orchestrate" a trusted cloud and restore needed transparency.
- Resist the temptation to jump into even a so-called “secure” cloud just to save money.
  - **Aim higher!**
  - **Jump into the right “trusted” cloud to create and capture new enterprise value.**



DIGITAL TRUST IN THE CLOUD

LIQUID SECURITY IN CLOUDY PLACES

CSC

EXPLORING SECURITY AND TRUST IN THE CLOUD

THE PAYOFF POTENTIAL OF DIGITAL TRUST IN CLOUD PROCESSING

CSC.COM

BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

RONALD B. KNODE, AUGUST 2009

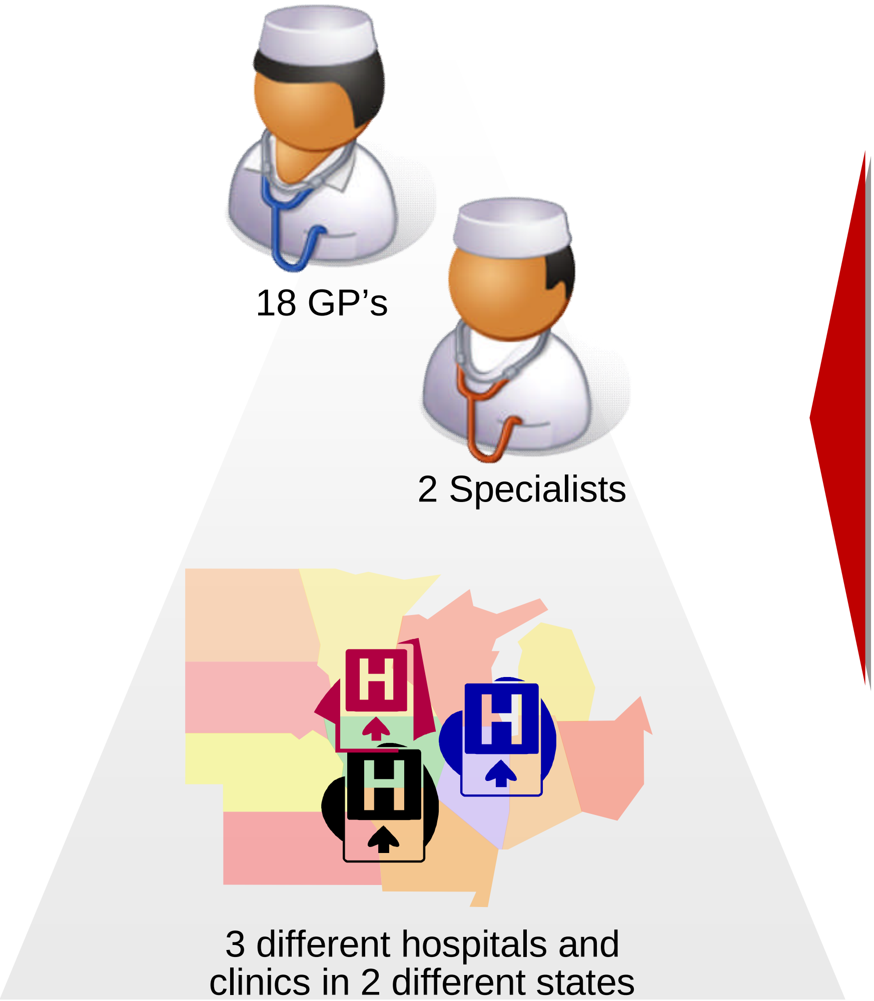
www.csc.com/security/insights/32270-digital_trust_in_the_cloud

Or at

www.csc.com/lefreports

Imagine This!

Medical practice



18 GP’s

2 Specialists

3 different hospitals and clinics in 2 different states

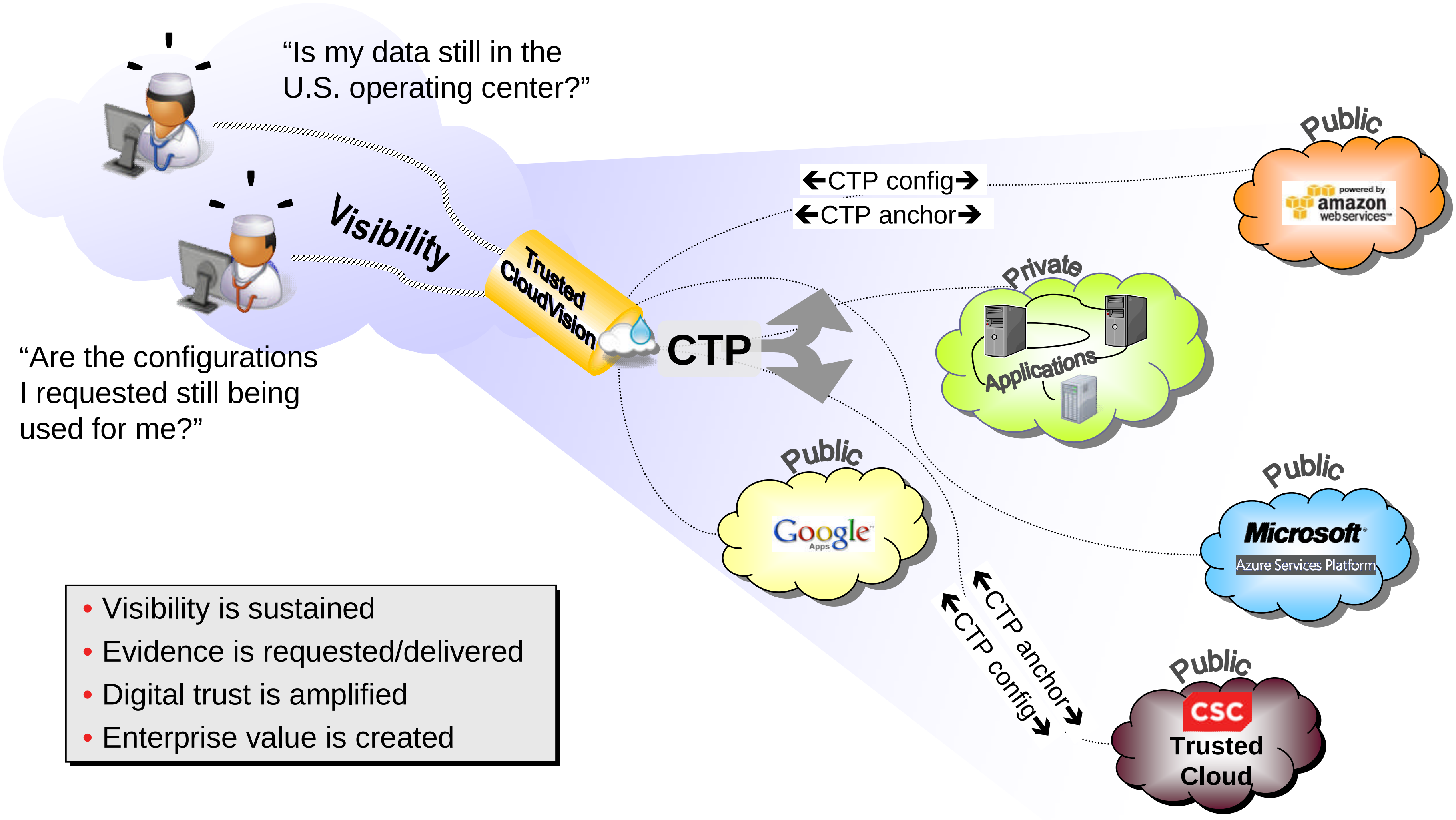
The Opportunity

- Public, “for profit” enterprise in the Midwest US
- Accept Medicare and Medicaid, … but only if ...
  - Major credit card to cover deductibles
- In-house electronic patient health record system (EHR)
  - Not certified by HHS
- Independent audits (financial and otherwise)
  - IT controls plan
  - Configuration specific
- Email and word processing assigned to public cloud already
- Desire to receive ARRA incentives for deploying fully certified EHR

The Payoff

- Double the size of the practice
- Reduce patient wait times
- Practice doctors spend 12% more time with patients
- Competitive advantage + Better care

CSC Trusted Cloud Services™ Make New Enterprise Value Possible



"Is my data still in the U.S. operating center?"

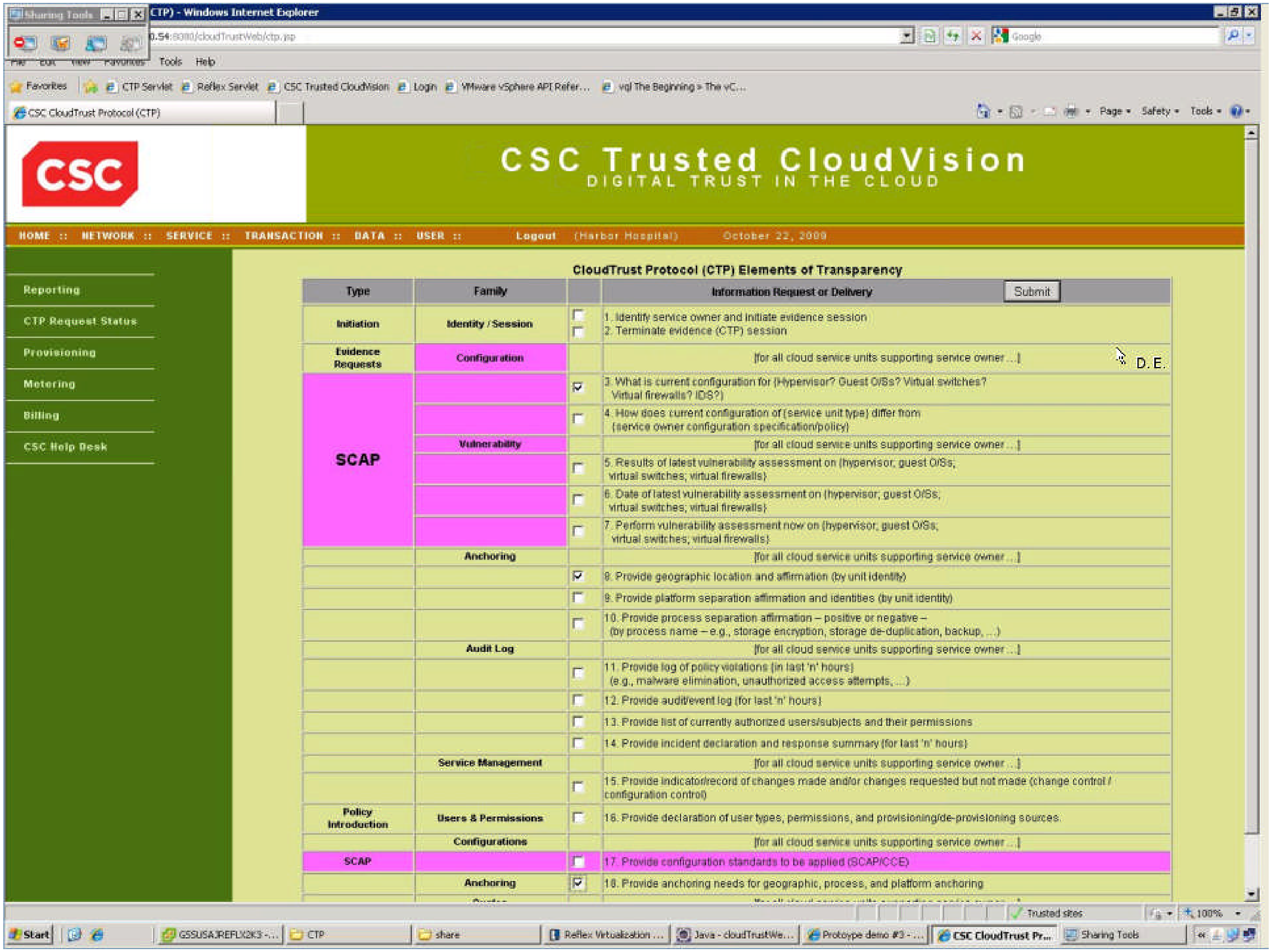
"Are the configurations I requested still being used for me?"

- Visibility is sustained
- Evidence is requested/delivered
- Digital trust is amplified
- Enterprise value is created

"… Right cloud. Right way."

CloudTrust Protocol in Action

Turning on the lights

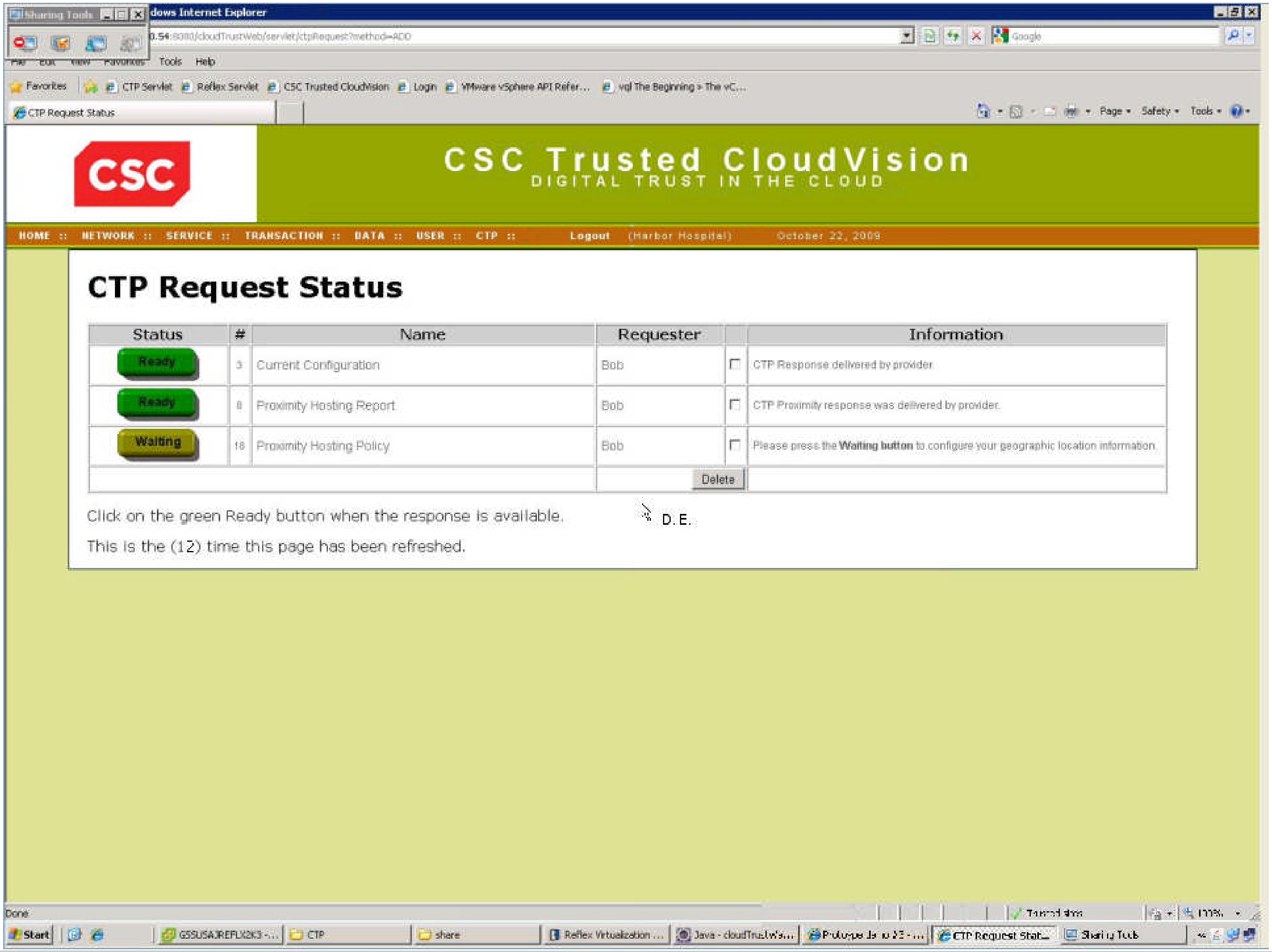

CTP) - Windows Internet Explorer
CSC CloudTrust Protocol (CTP)
CSC
CSC Trusted CloudVision
DIGITAL TRUST IN THE CLOUD
HOME :: NETWORK :: SERVICE :: TRANSACTION :: DATA :: USER ::
Logout (Harbor Hospital) October 22, 2009
Reporting
CTP Request Status
Provisioning
Metering
Billing
CSC Help Desk
D. E.

CloudTrust Protocol (CTP) Elements of Transparency

Type	Family		Information Request or Delivery Submit
Initiation	Identity / Session	□ □	1. Identify service owner and initiate evidence session 2. Terminate evidence (CTP) session
Evidence Requests	Configuration		[for all cloud service units supporting service owner ...]
SCAP		☑	3. What is current configuration for {Hypervisor? Guest O/Ss? Virtual switches? Virtual firewalls? IDS?}
		□	4. How does current configuration of {service unit type} differ from {service owner configuration specification/policy}
	Vulnerability		[for all cloud service units supporting service owner ...]
		□	5. Results of latest vulnerability assessment on {hypervisor; guest O/Ss; virtual switches; virtual firewalls}
		□	6. Date of latest vulnerability assessment on {hypervisor; guest O/Ss; virtual switches; virtual firewalls}
		□	7. Perform vulnerability assessment now on {hypervisor; guest O/Ss; virtual switches; virtual firewalls}
	Anchoring		[for all cloud service units supporting service owner ...]
		☑	8. Provide geographic location and affirmation (by unit identity)
		□	9. Provide platform separation affirmation and identities (by unit identity)
		□	10. Provide process separation affirmation – positive or negative – (by process name – e.g., storage encryption, storage de-duplication, backup, ...)
	Audit Log		[for all cloud service units supporting service owner ...]
		□	11. Provide log of policy violations {in last 'n' hours} (e.g., malware elimination, unauthorized access attempts, ...)
		□	12. Provide audit/event log {for last 'n' hours}
		□	13. Provide list of currently authorized users/subjects and their permissions
		□	14. Provide incident declaration and response summary {for last 'n' hours}
	Service Management		[for all cloud service units supporting service owner ...]
		□	15. Provide indicator/record of changes made and/or changes requested but not made (change control / configuration control)
Policy Introduction	Users & Permissions	□	16. Provide declaration of user types, permissions, and provisioning/de-provisioning sources.
	Configurations		[for all cloud service units supporting service owner ...]
SCAP		□	17. Provide configuration standards to be applied (SCAP/CCE)
	Anchoring	☑	18. Provide anchoring needs for geographic, process, and platform anchoring

CloudTrust Protocol in Action

Checking the lights



CTP Request Status

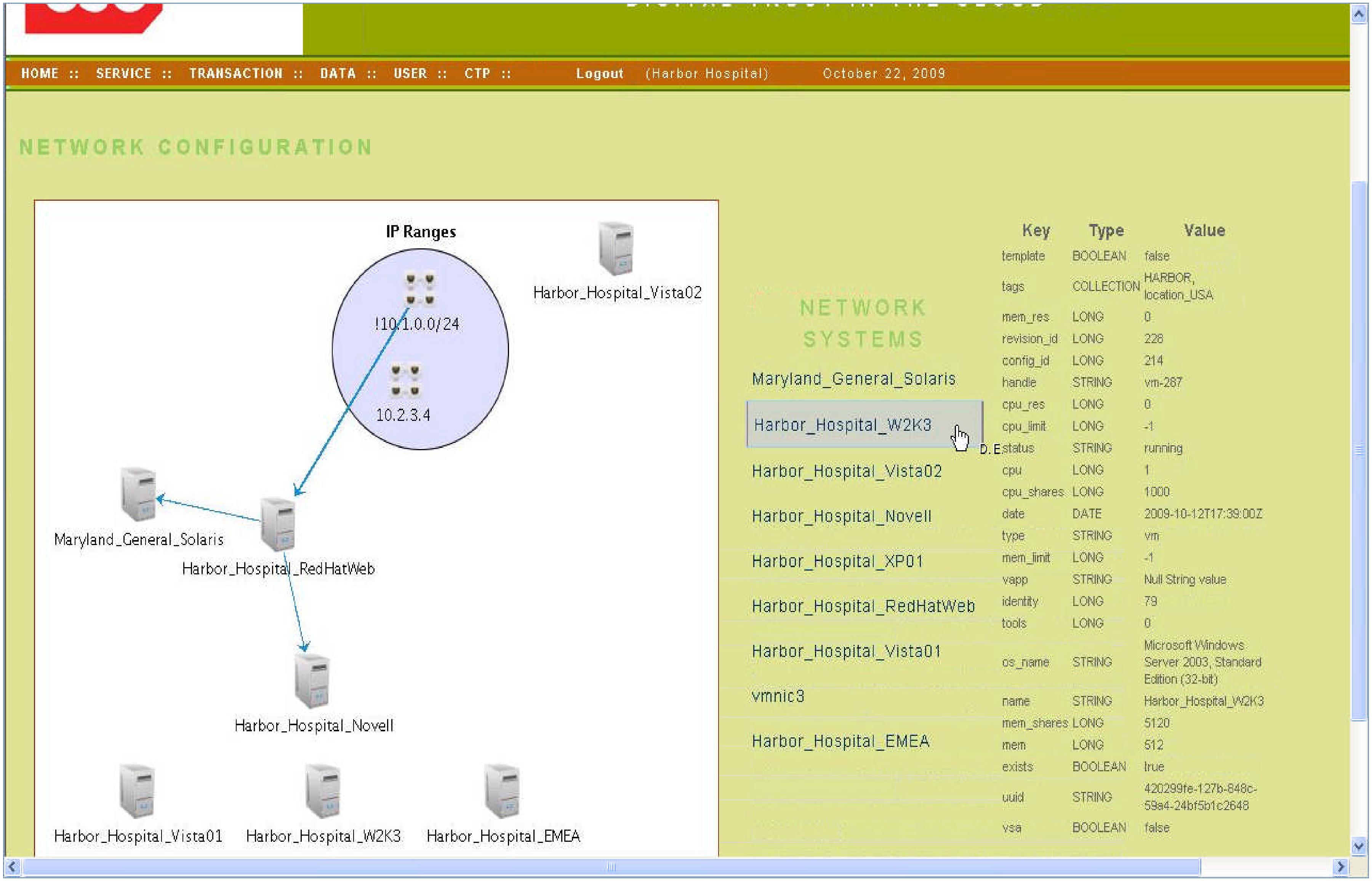
Status	#	Name	Requester		Information
Ready	3	Current Configuration	Bob	□	CTP Response delivered by provider.
Ready	8	Proximity Hosting Report	Bob	□	CTP Proximity response was delivered by provider.
Waiting	16	Proximity Hosting Policy	Bob	□	Please press the **Waiting button** to configure your geographic location information.
			Delete		

Click on the green Ready button when the response is available.

D. E.

This is the (12) time this page has been refreshed.

SCAP-based Configuration Request and Reply



NETWORK CONFIGURATION

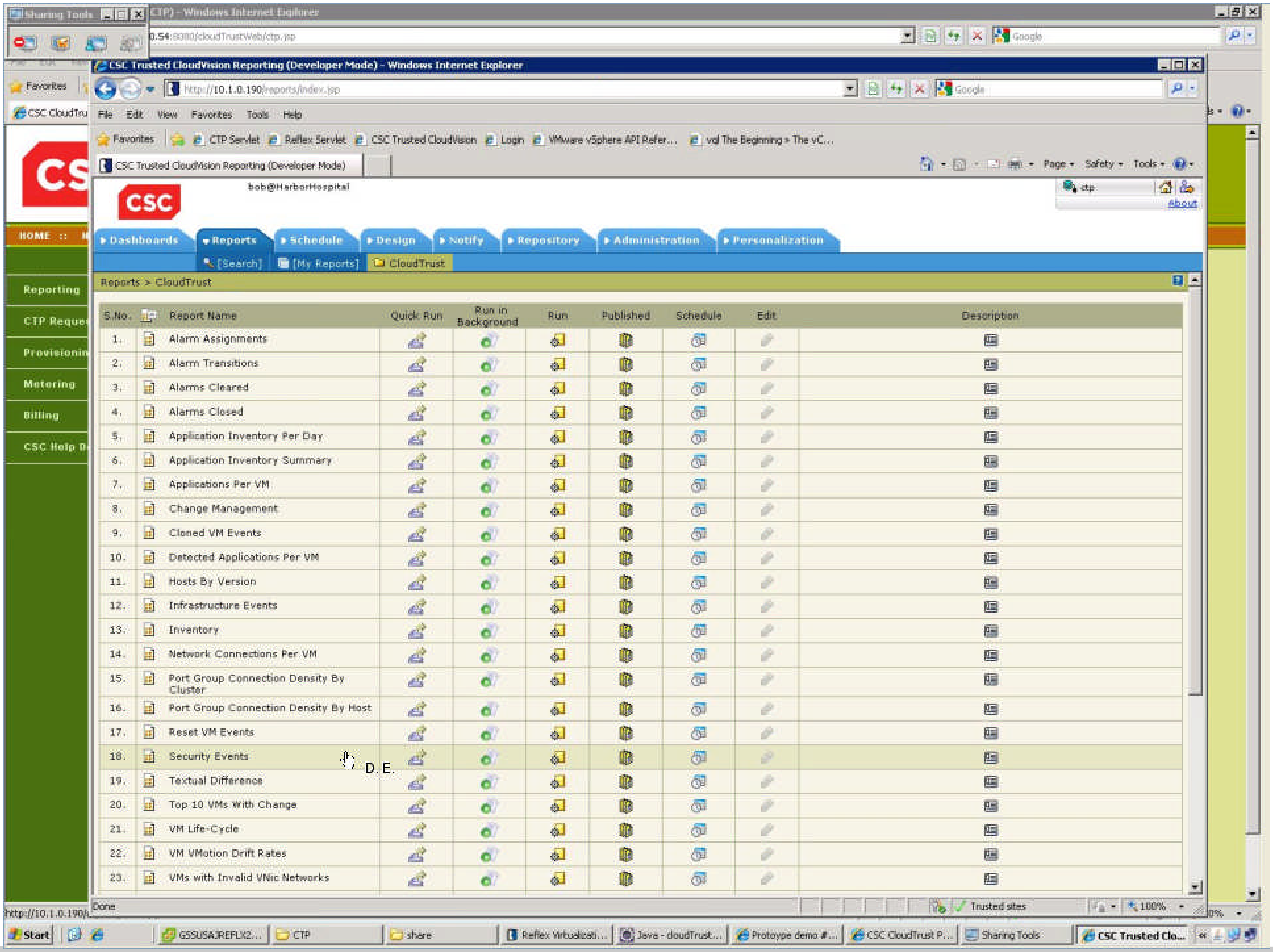
NETWORK SYSTEMS

- Maryland_General_Solaris
- Harbor_Hospital_W2K3
- Harbor_Hospital_Vista02
- Harbor_Hospital_Novell
- Harbor_Hospital_XP01
- Harbor_Hospital_RedHatWeb
- Harbor_Hospital_Vista01
- vmnic3
- Harbor_Hospital_EMEA

Key	Type	Value
template	BOOLEAN	false
tags	COLLECTION	HARBOR, location_USA
mem_res	LONG	0
revision_id	LONG	228
config_id	LONG	214
handle	STRING	vm-287
cpu_res	LONG	0
cpu_limit	LONG	-1
status	STRING	running
cpu	LONG	1
cpu_shares	LONG	1000
date	DATE	2009-10-12T17:39:00Z
type	STRING	vm
mem_limit	LONG	-1
vapp	STRING	Null String value
identity	LONG	79
tools	LONG	0
os_name	STRING	Microsoft Windows Server 2003, Standard Edition (32-bit)
name	STRING	Harbor_Hospital_W2K3
mem_shares	LONG	5120
mem	LONG	512
exists	BOOLEAN	true
uuid	STRING	420299fe-127b-848c-59a4-24bf5b1c2648
vsa	BOOLEAN	false

CloudTrust Protocol in Action

All the lights to check



S.No.	Report Name
1.	Alarm Assignments
2.	Alarm Transitions
3.	Alarms Cleared
4.	Alarms Closed
5.	Application Inventory Per Day
6.	Application Inventory Summary
7.	Applications Per VM
8.	Change Management
9.	Cloned VM Events
10.	Detected Applications Per VM
11.	Hosts By Version
12.	Infrastructure Events
13.	Inventory
14.	Network Connections Per VM
15.	Port Group Connection Density By Cluster
16.	Port Group Connection Density By Host
17.	Reset VM Events
18.	Security Events
19.	Textual Difference
20.	Top 10 VMs With Change
21.	VM Life-Cycle
22.	VM VMotion Drift Rates
23.	VMs with Invalid VNic Networks

You Can Help

Are we at the fraying ends of a fad, or the beginning of a bonanza of IT value and performance?

- Secure cloud processing must offer more than just economy.
  - *Security* in the cloud is not enough
  - *Trust* in the cloud is necessary to create new enterprise value

- Partnership with government agencies and service and technology enterprises to solidify standards is necessary and inevitable.

- Join the cloud standards community of the OMG to help complete the open definition and application of cloud standards, including CloudTrust!

- Do not wait too long ... participate with your own cloud pilots for yourselves as well as your own communities … *Things are looking up!*

Clouds Come with Rainbows

- Visibility brings trust
- Trust brings payoffs
- CloudTrust elements of transparency let everyone deliver visibility
- Join the OMG effort and help complete the definition