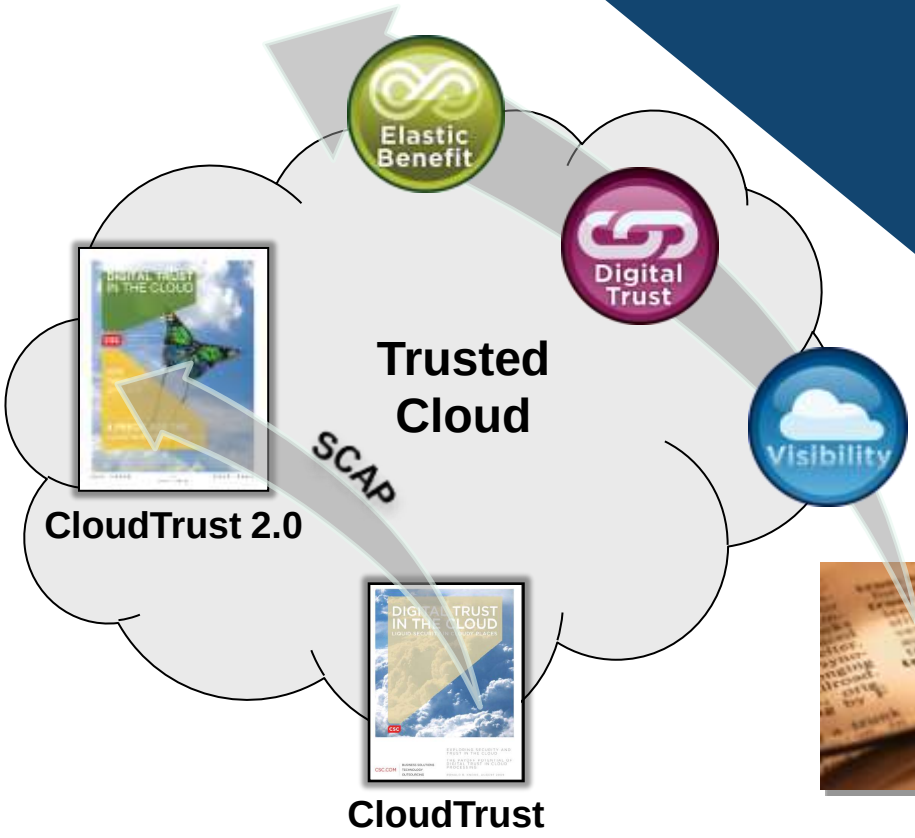
CloudTrust 2.0

In the Cloud, 'Security' Starts with a 'T'

Lubricating digital trust in the cloud with SCAP

28 September 2010

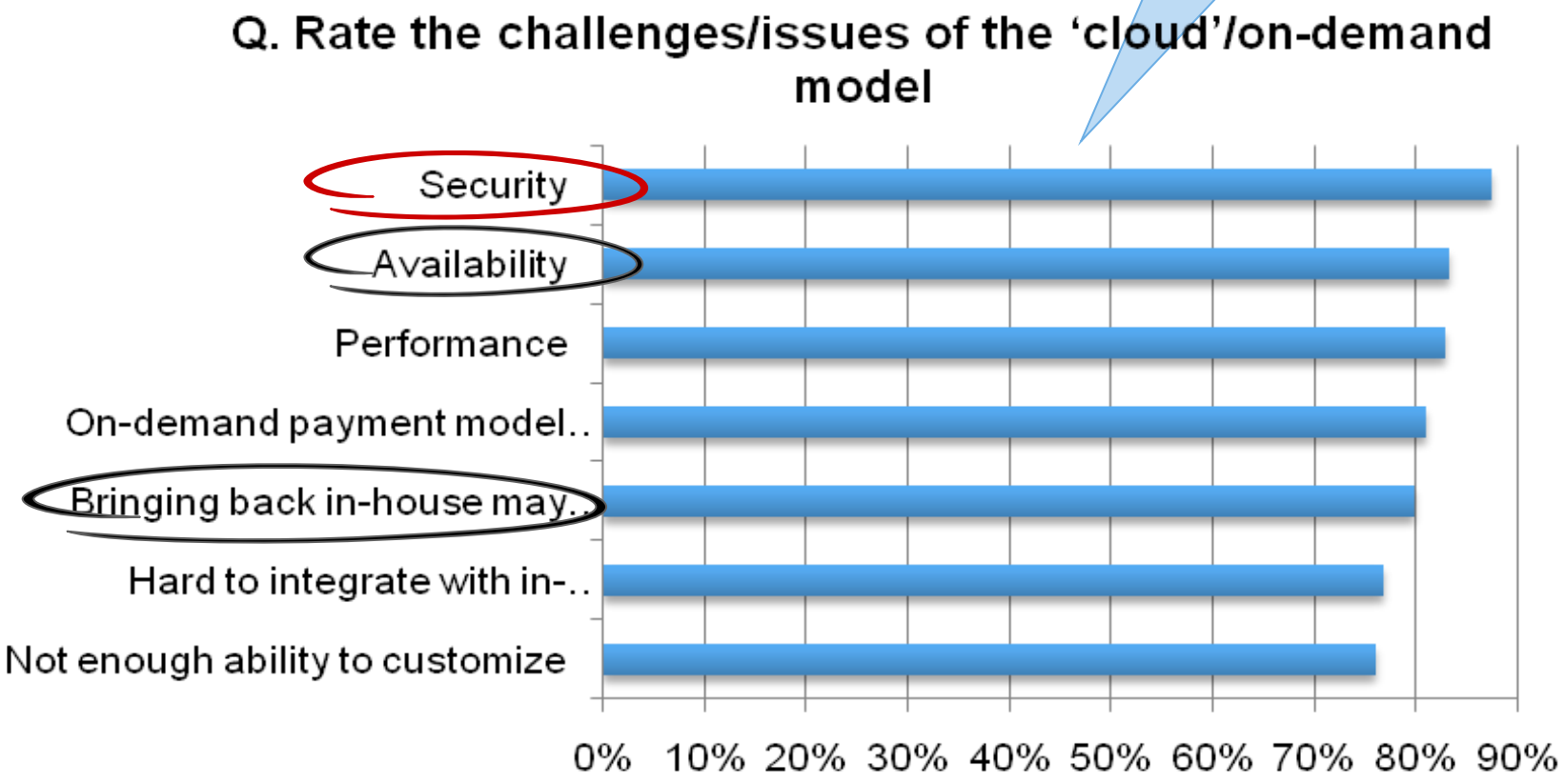


Ron Knode

Provocative … Attractive … Sometimes Effective … But …

The Dark Side

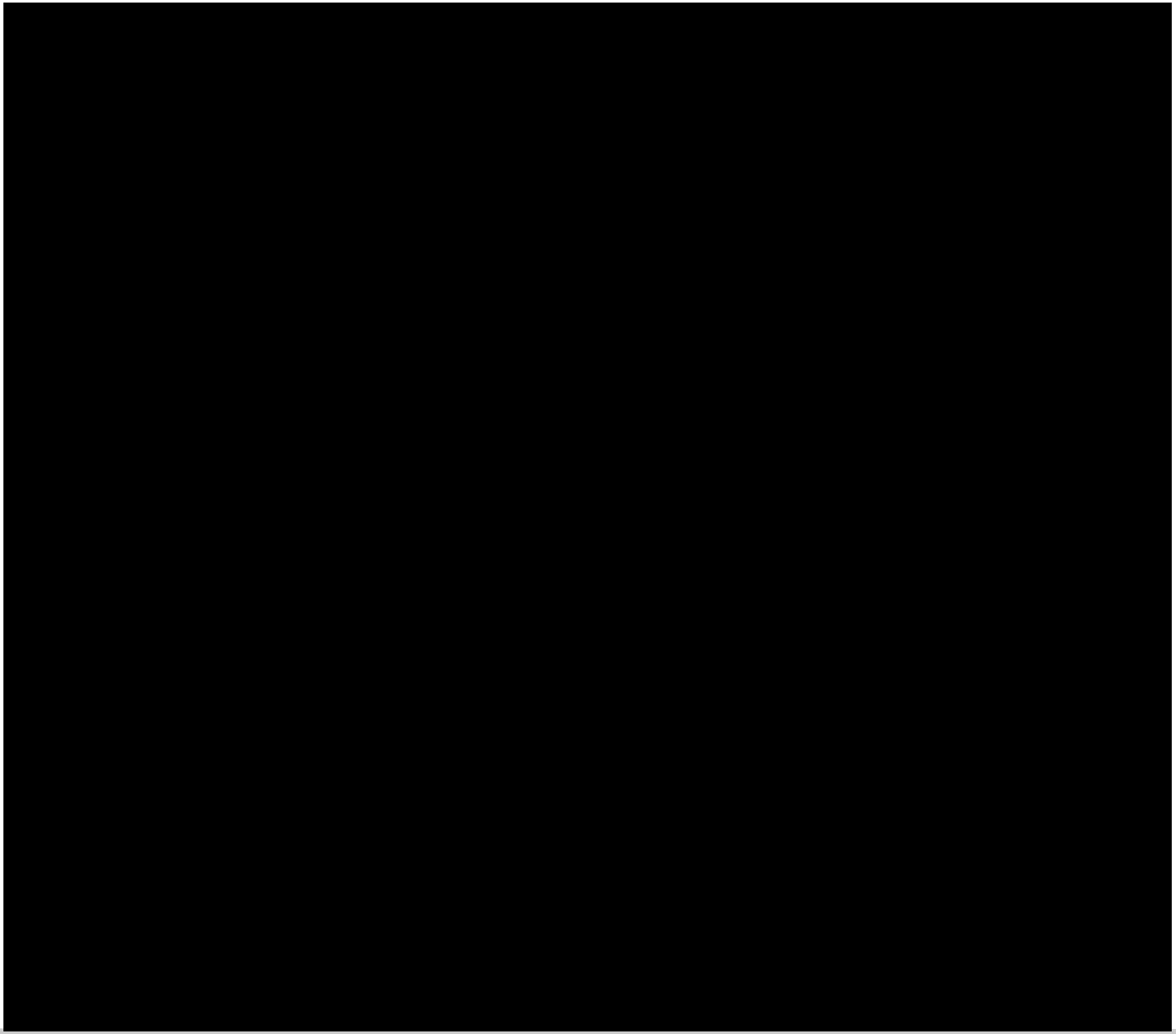
Pick your survey … any survey … they all look like this!



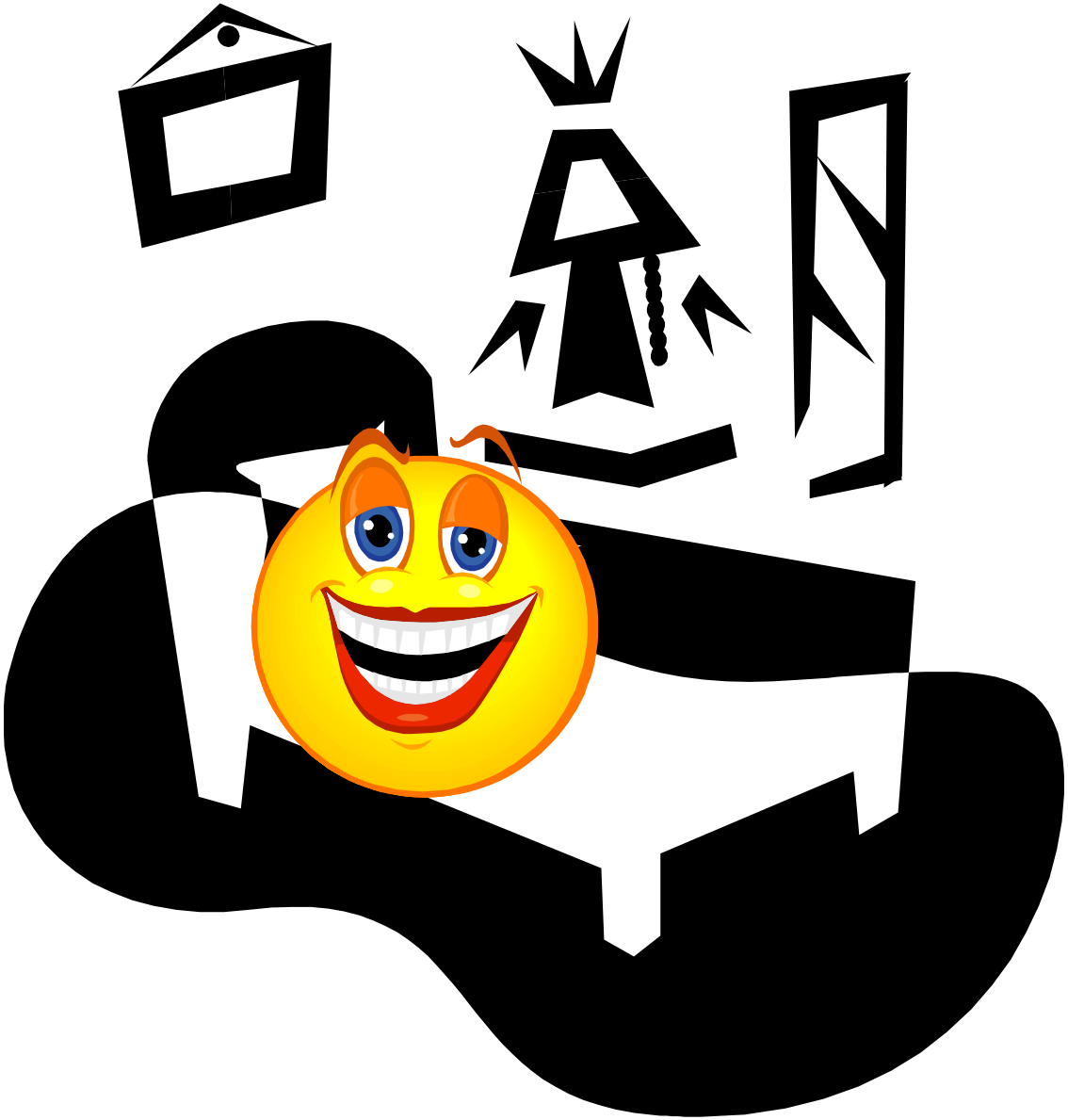
*Scale: 1= Not at all concerned 5=Very concerned

Source: IDC Enterprise Panel, 3Q 09.n=263, September 2009

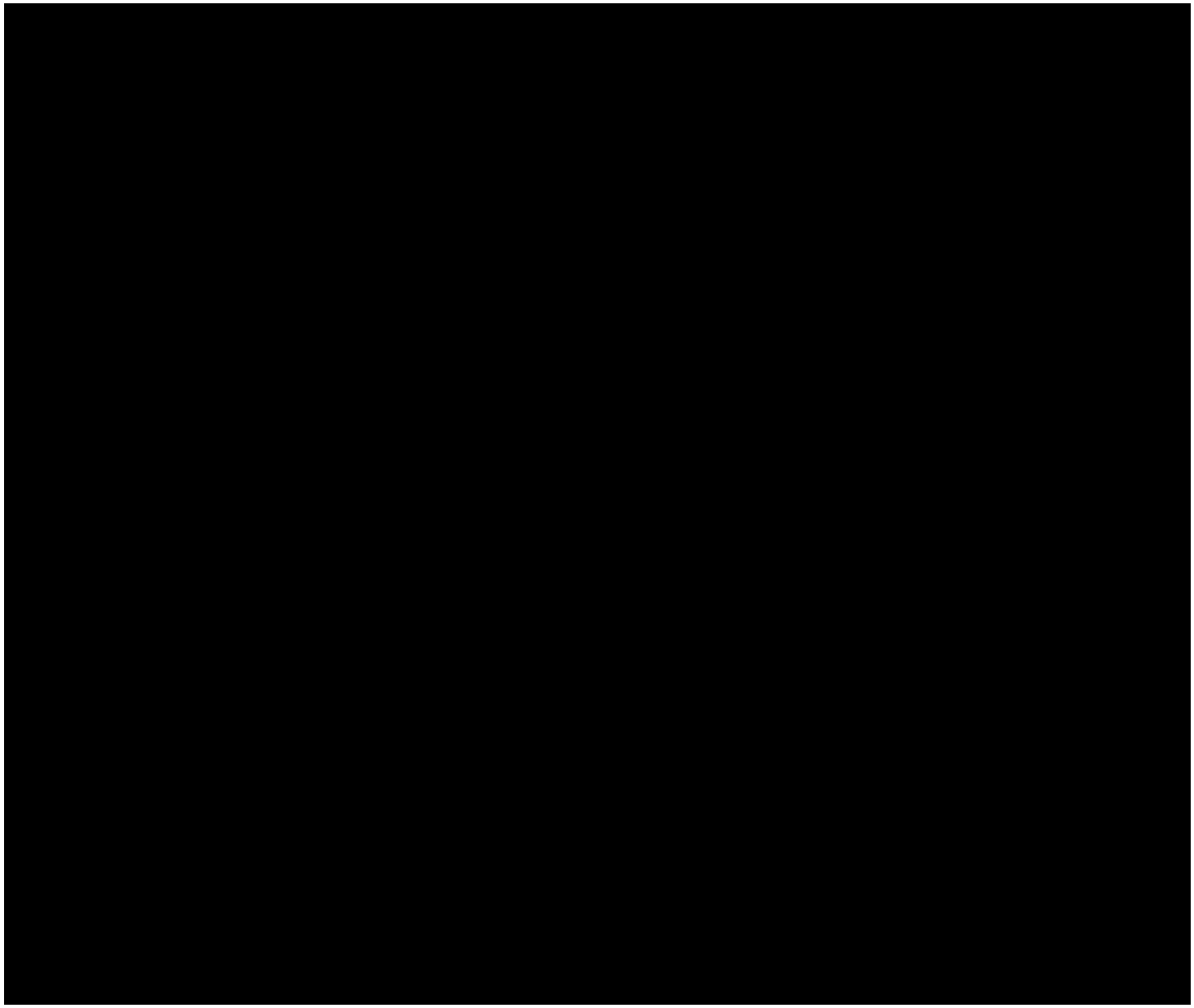
Are You Afraid of the Dark?



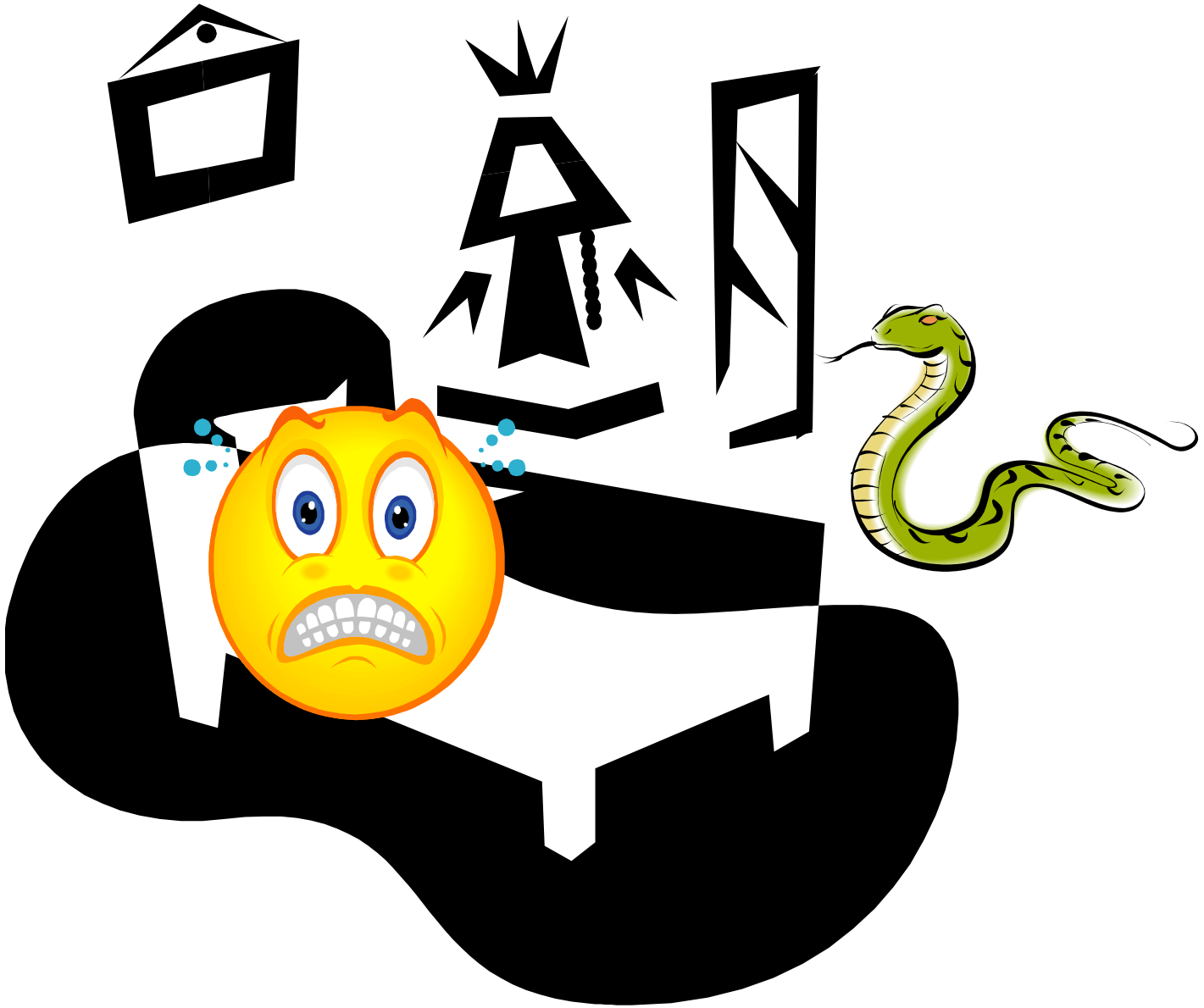
Are You Afraid of the Dark?



Are You Afraid of the Dark?



Are You Afraid of the Dark?



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 …,

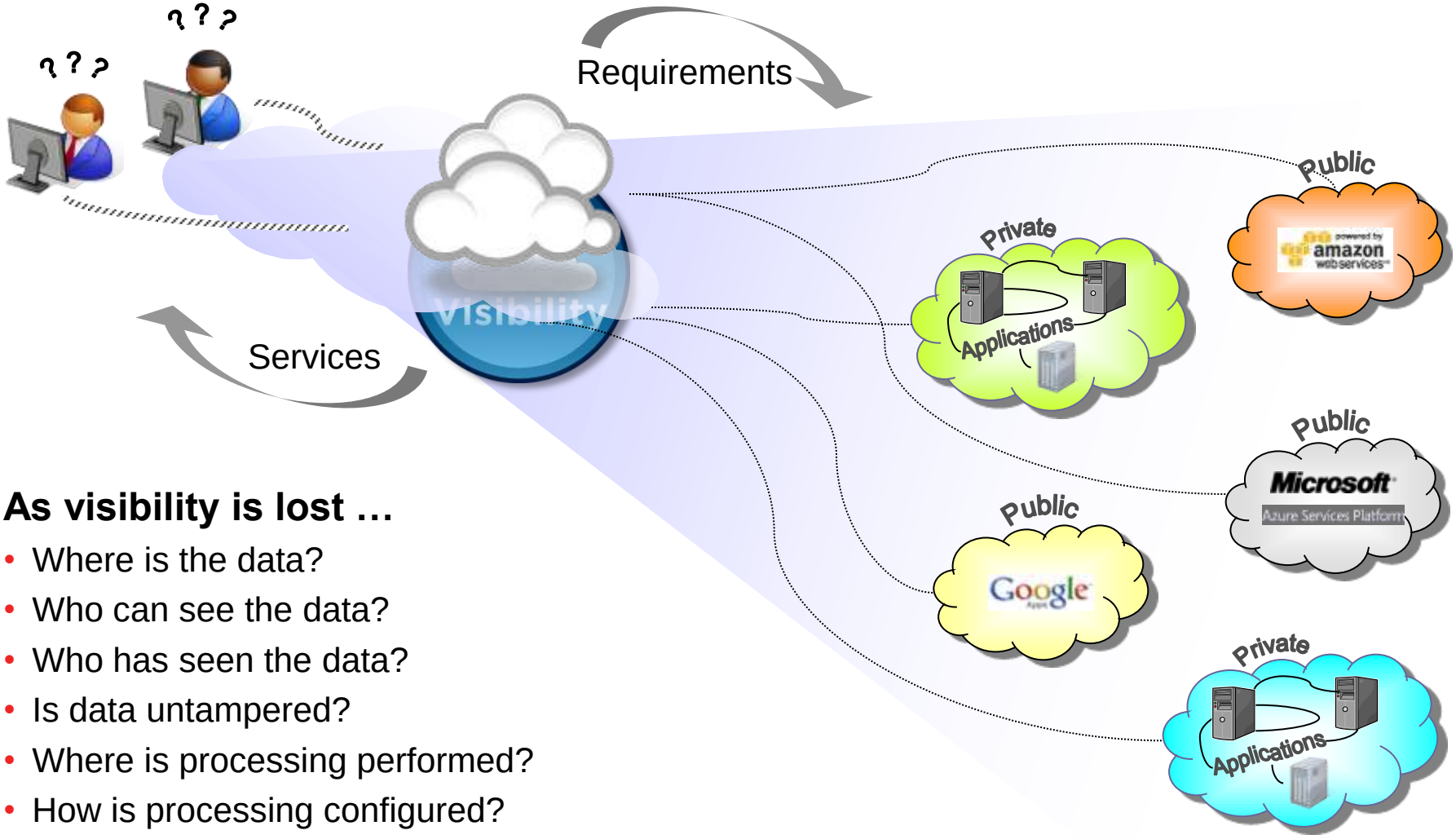
Compliance issues

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

… and on and on and on …

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

Absent Transparency … Some Big Problems

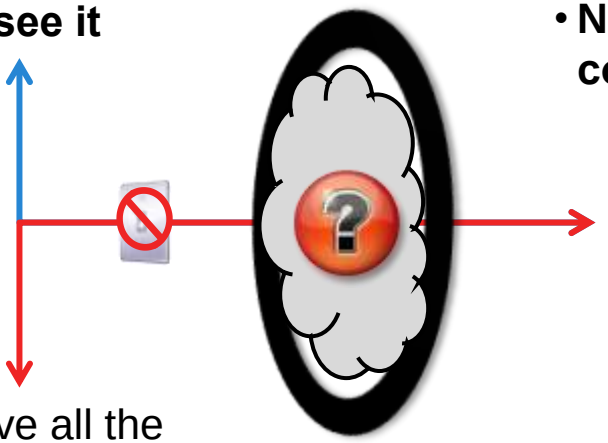
For example, … without transparency …

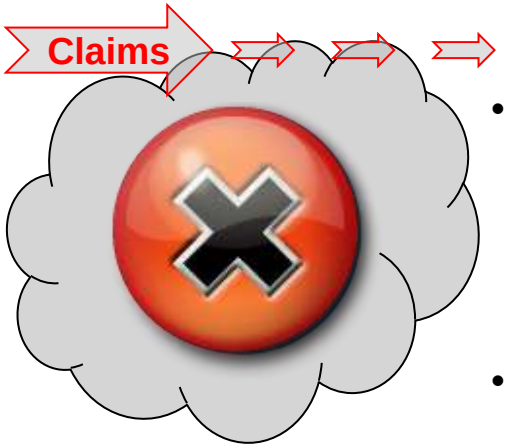
- No confirmed chain of custody for information
- No way to conduct investigative forensics
- Little confidence in the ability to detect attempts or occurrences of illegal disclosure
- Little capability to discover or enforce configurations
- No ability to monitor operational access or service management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

The Cloud Security Paradox
Without transparency value is lost either way!

- I really do have all the security & privacy technologies and services I claim, and they are working now for you
- **You can't see it**

- **No Transparency?!**
- **No evidence-based confidence …!!**





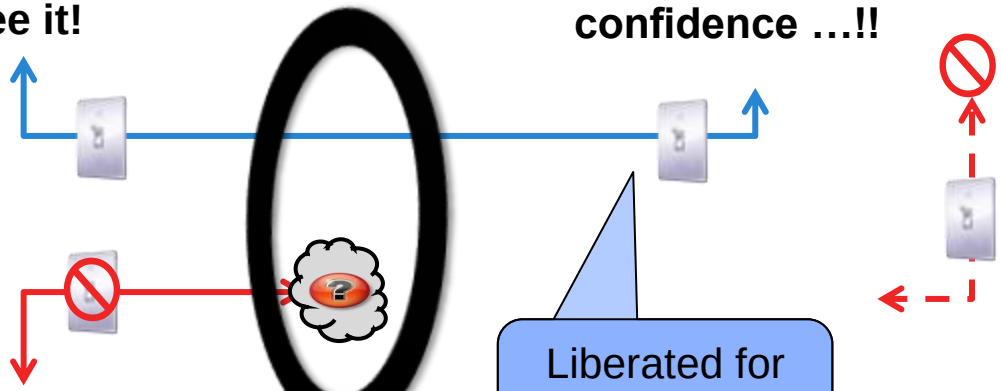
- I do not have all the security & privacy technologies and services I claim, or they are not working now for you
- **You can't see it**

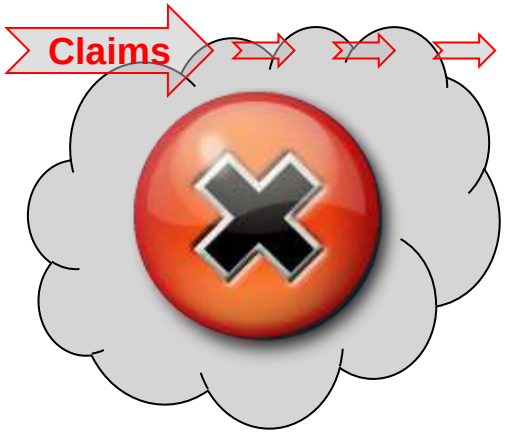
Payoffs Denied

Cloud Security Starts with a 'T'
Transparency liberates value opportunities

- I really do have all the security & privacy technologies and services I claim, and they are working now for you
- **You can see it!**

- **Transparency!!**
- **Evidence-based confidence …!!**



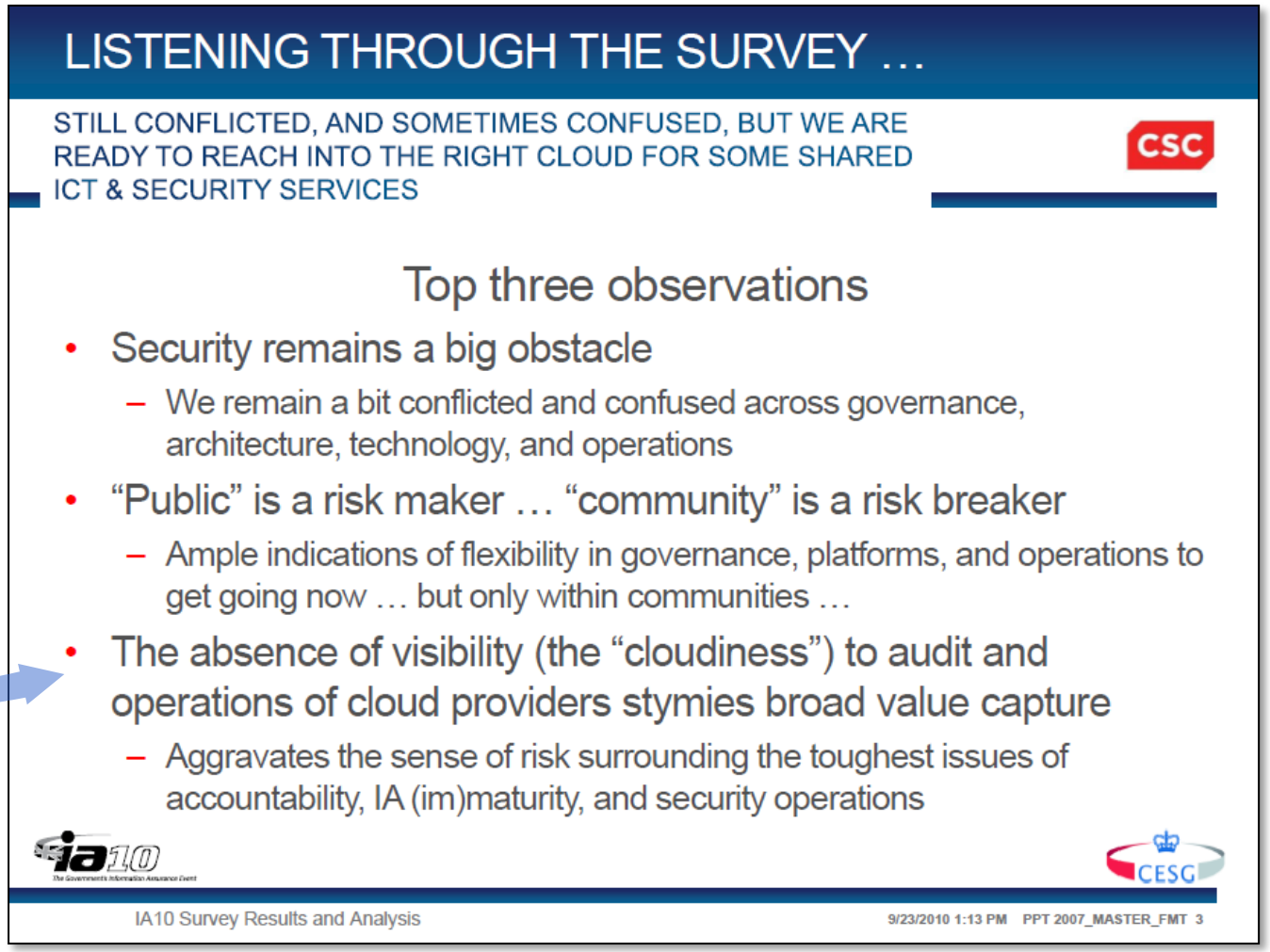


- I do not have all the security & privacy technologies and services I claim, or they are not working now for you
- **You can see it or visibility is denied**

Liberated for New Payoffs!

Transparency in the Cloud is (still) the Key to Value Capture

- United Kingdom IA10 Conference (13-15 Sept 2010)
- Top security policy makers and providers in the UK (gov't and industry)
- Transparency is acknowledged (again) as the key to value capture



The Real Value Question for Cloud Processing

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

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

Without disqualifying any cloud provider or consumer … ?!

Weatherproofing the Enterprise for Cloud Services

Transparency (monitoring) to create digital trust

Today – Compensating Approaches

Private Clouds

"Safe Computing" for Cloud Processing

Presumptive Security

Coming – Reclaiming Transparency

Transparency Services

Protocols

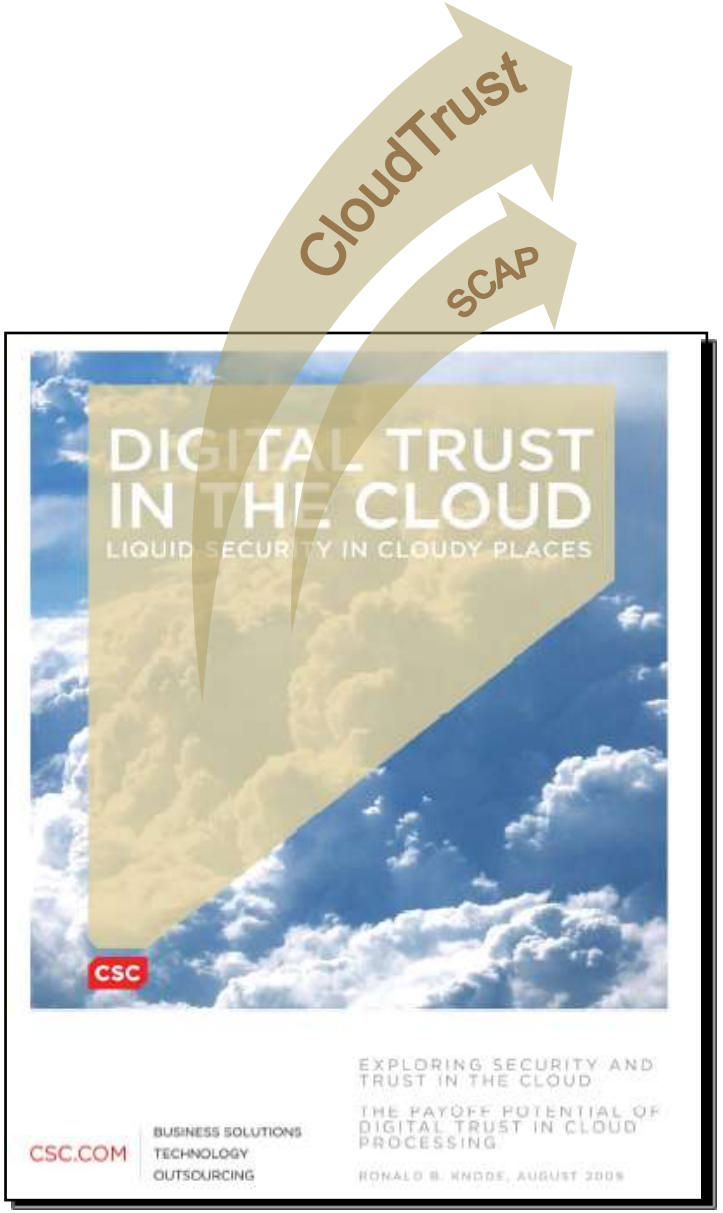
Standards

Audits

Standards-based continuous monitoring with a purpose

Research Conclusions Summary
July 2009

- 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.**

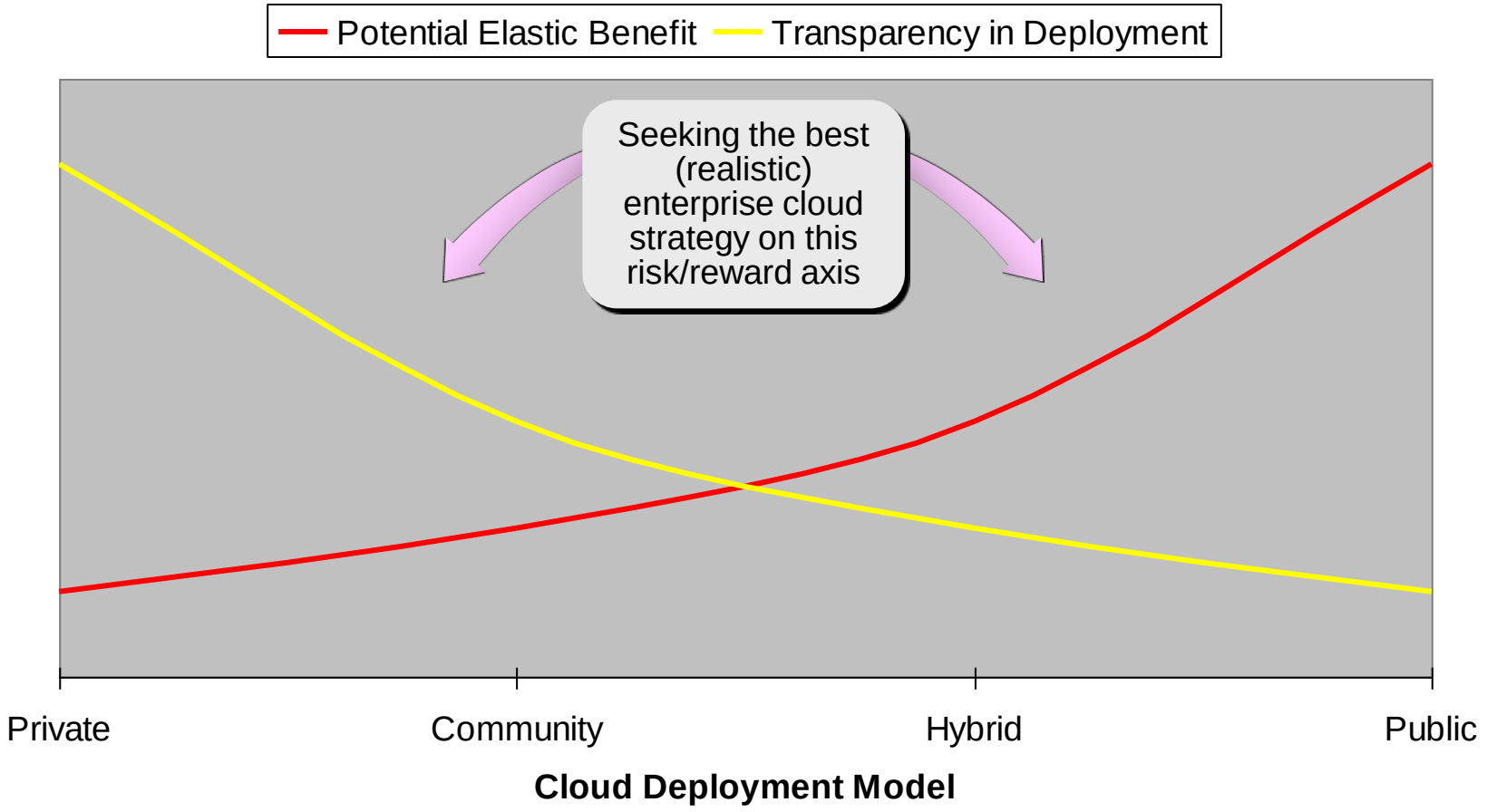


www.csc.com/security/insights/32270-digital_trust_in_the_cloud

Or at

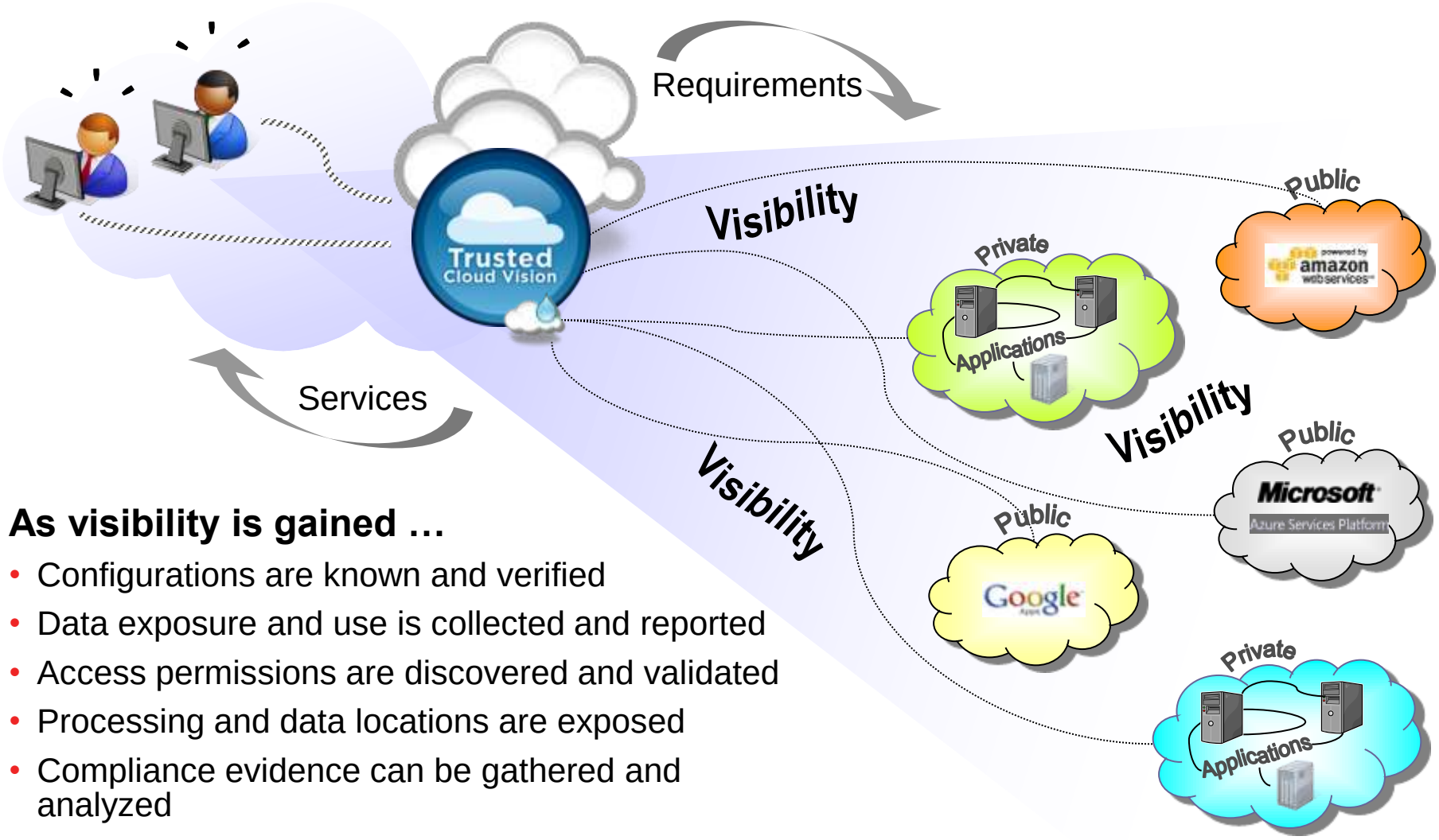
www.csc.com/lefreports

Using Transparency to Ride the Payoff Curve
More applications and services become eligible for the cloud



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

A “Trusted” Cloud

- A Cloud

  …..that harmonizes the security for transactions and data

  with

  ……comprehensive transparency of control and result

  such that

  ……it conveys evidence-based confidence that systems within its environment operate as advertised, and that no unadvertised functions are occurring*

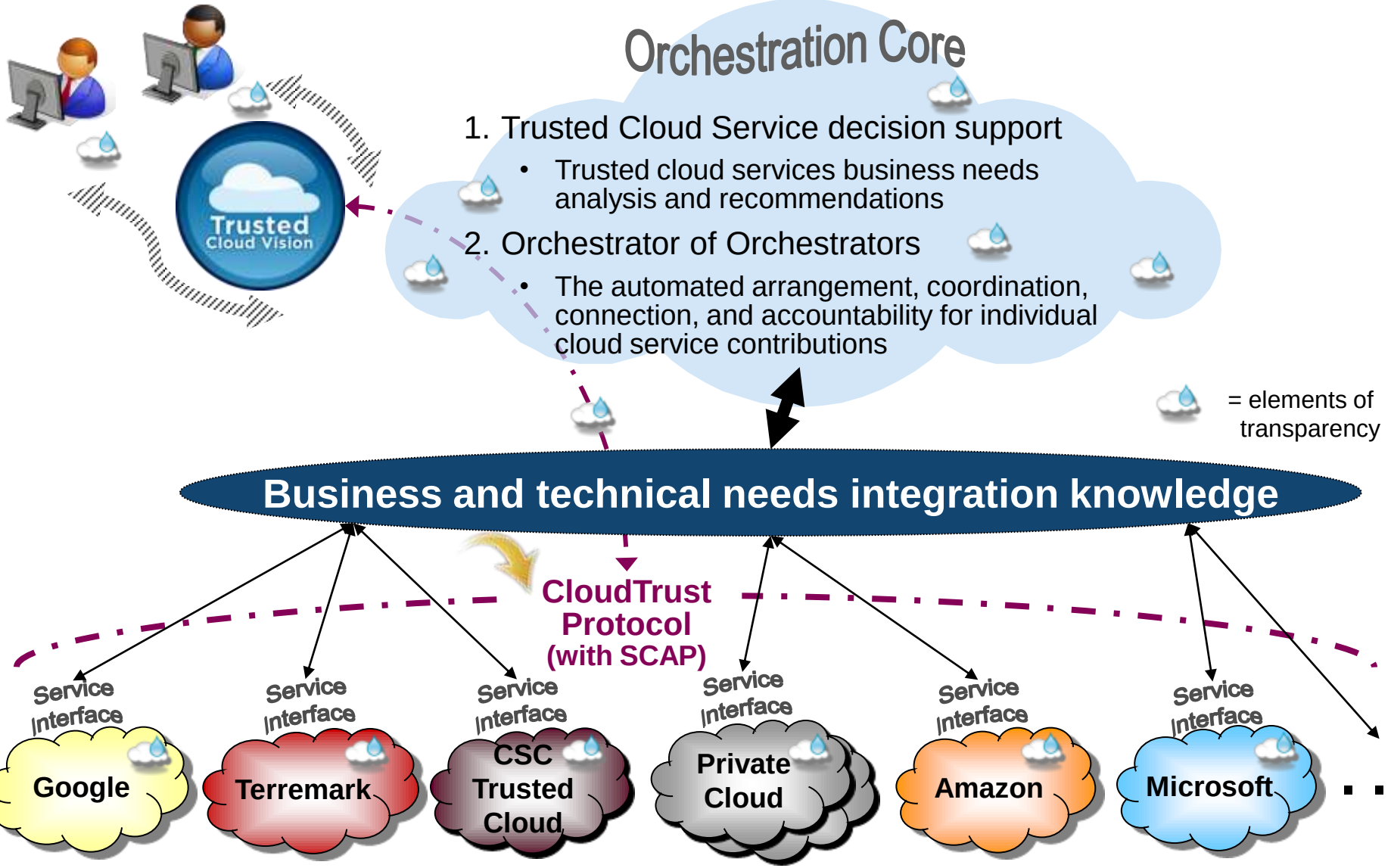
is a Trusted Cloud

- Services rendered via a Trusted Cloud are “Trusted Cloud Services”

The generation of new enterprise value with Trusted Cloud Services is an application of Digital Trust

*See: The LEF series “Digital Trust: Shaking Hands with the Digital Enterprise” www.csc.com/lefreports

Important Part of Cloud Orchestration & Management
Translation of Business Needs to Trusted Cloud Service Delivery



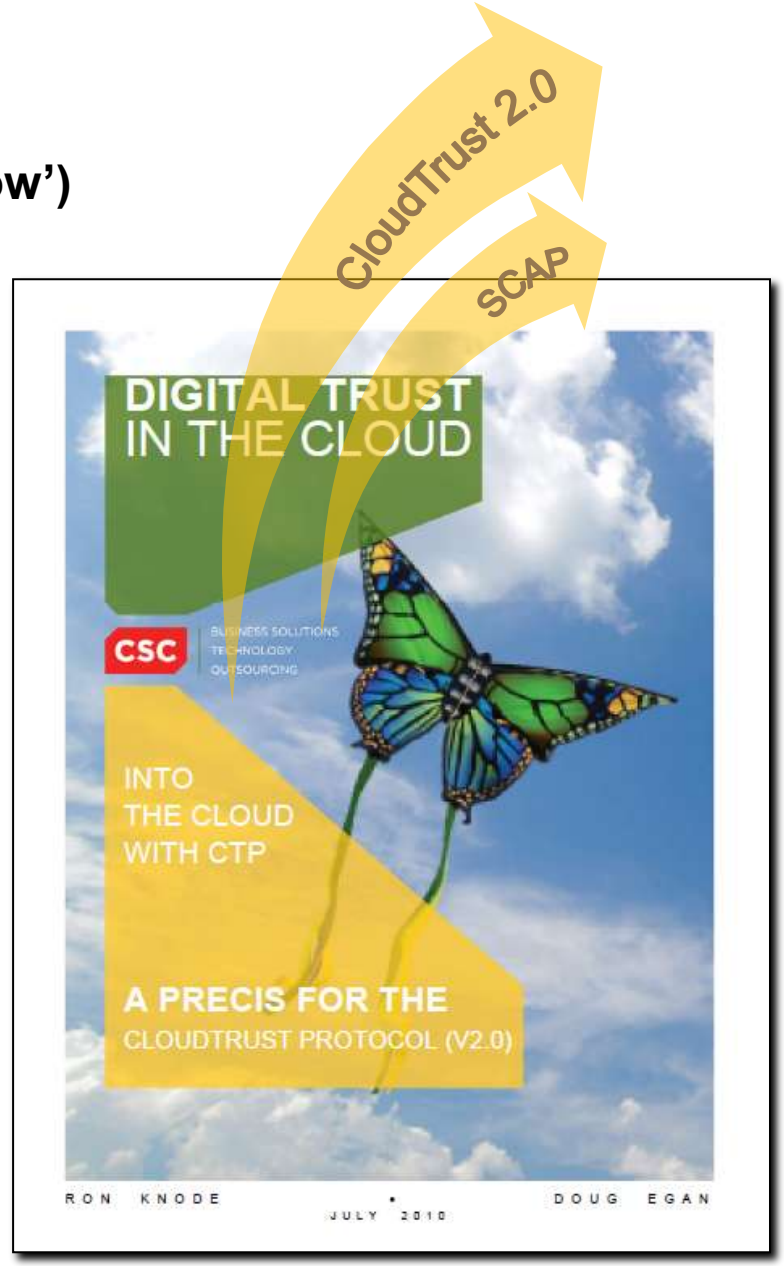
Trusted CloudVision™
CloudTrust Protocol (CTP) Activation Sample

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 …

CloudTrust Protocol Revealed
(Research extension detailing 'what' and 'how')

- Transparency in the cloud is the key to capturing digital trust payoffs for both cloud consumers and cloud providers.
- The CloudTrust Protocol (CTP) offers an uncomplicated, natural way to request and receive fundamental information about essential elements of transparency.
- The reliable delivery of only a few elements of transparency generate a lot of digital trust, and that digital trust liberates cloud users to bring more and more core enterprise services and data to cloud techniques.
- Transparency-as-a-Service (TaaS) using the CTP provides a flexible, uniform, and simple technique for reclaiming transparency into actual cloud architectures, configurations, services, and status … responding to both cloud user and cloud provider needs.
- Transparency protocols like the CTP must be accompanied by corresponding concepts of operation and contractual conditions to be completely effective.



http://www.trustedcloudservices.com/images/stories/pdf_downloads/wp-cloudtrustprotocolprecis-073010.pdf

A Handbook for CTP Implementation – Deployment – Use
Continuous Trust Monitoring in the Cloud

- Business value analysis
- Expansion of CTP to V2.0
- Dimensions of flexibility in implementation and use
  - Adaptability in asset model
  - Scope of response (“I refuse” is OK; the CloudTrust Index)
  - Context of deployment (orchestration or standalone)
  - Scope of coverage (enterprise or client-specific)
  - Level of automation and protocol conveyance (in-band or out-of-band)
- Elements of transparency (V2.0) – full syntax and semantics
- Operational recommendations
  - Service Level Agreements
  - Concept of Operations

- Continuous monitoring for the cloud consumer
- Standard response mechanism for the cloud provider

Elements of Transparency in the CTP V2.0

- 6 Types
  - Initiation
  - Policy Introduction
  - Provider assertions
  - Provider notifications
  - Evidence requests
  - Client extensions

- Families
  - Configuration
  - Vulnerabilities
  - **Anchoring**
  - Audit log
  - Service Management
  - Service Statistics

Only 23 in total in the entire protocol!

- Elements
  - Geographic
  - Platform
  - Process

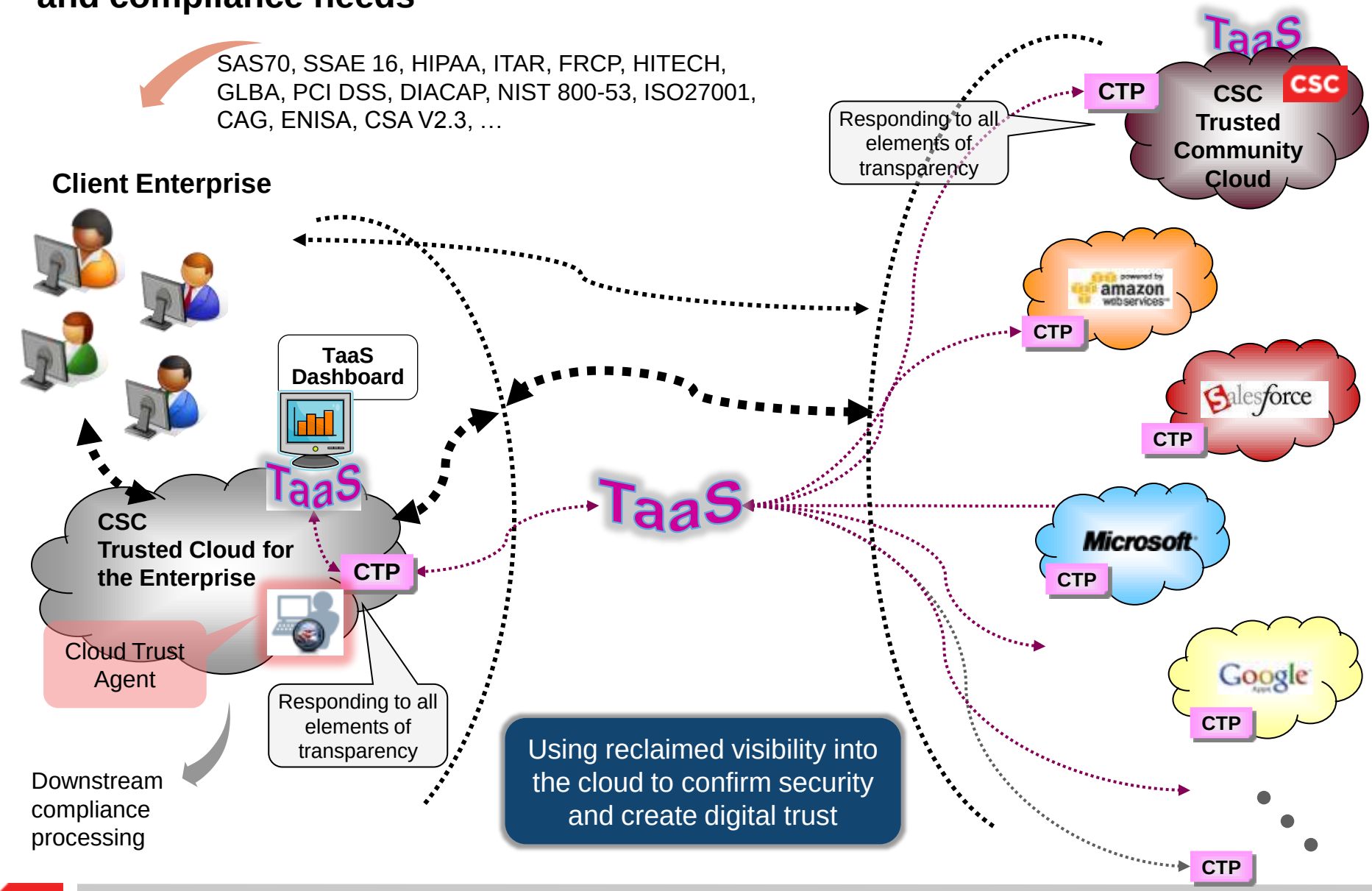
CloudTrust Protocol Pathways
Mapping the Elements of Transparency in Deployment

Admin & Ops	Specs	Transparency Requests			Extensions
		Assertions	**Evidence**	**Affirmations**	
	Configuration definition: 20	Security capabilities and operations:17	Configuration & vulnerabilities: 3,4,5,6,7	Anchoring: 8, 9, 10 (geographic, platform, process)	
	SCAP	**CloudAudit.org**	**SCAP**	**Sign / sealing**	
Session start: 1 Session end: 2 Alerts: 18	Users: 19 Anchors: 21 Quotas: 22 Alert conditions: 23		Violation: 11 Audit: 12 Access: 13 Incident log: 14 Config/control: 15 Stats: 16		Consumer/provider negotiated: 24

23 1

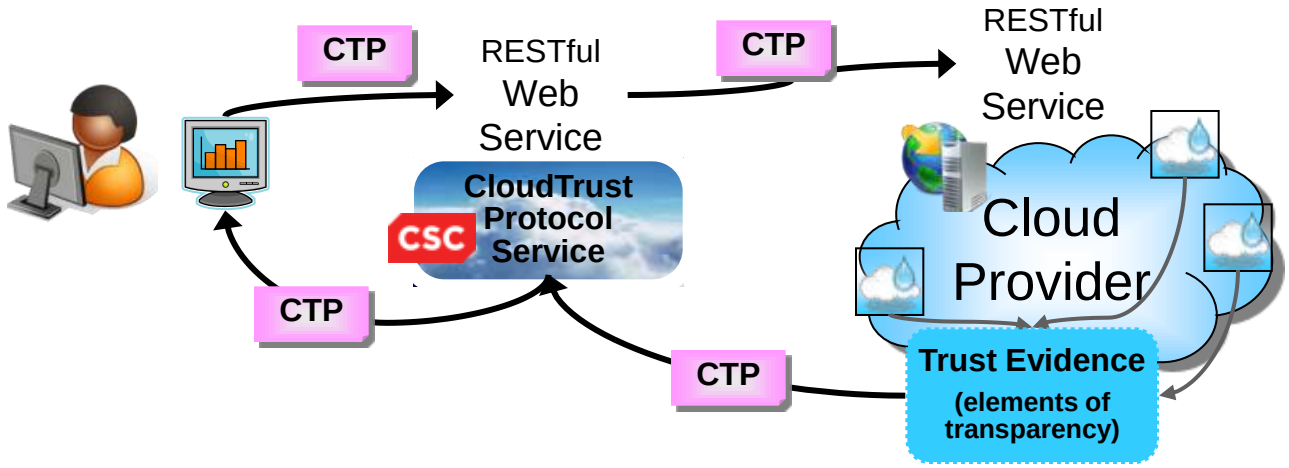
CloudTrust Protocol Transparency as a Service (TaaS)

Reclaiming digital trust across security, privacy, and compliance needs

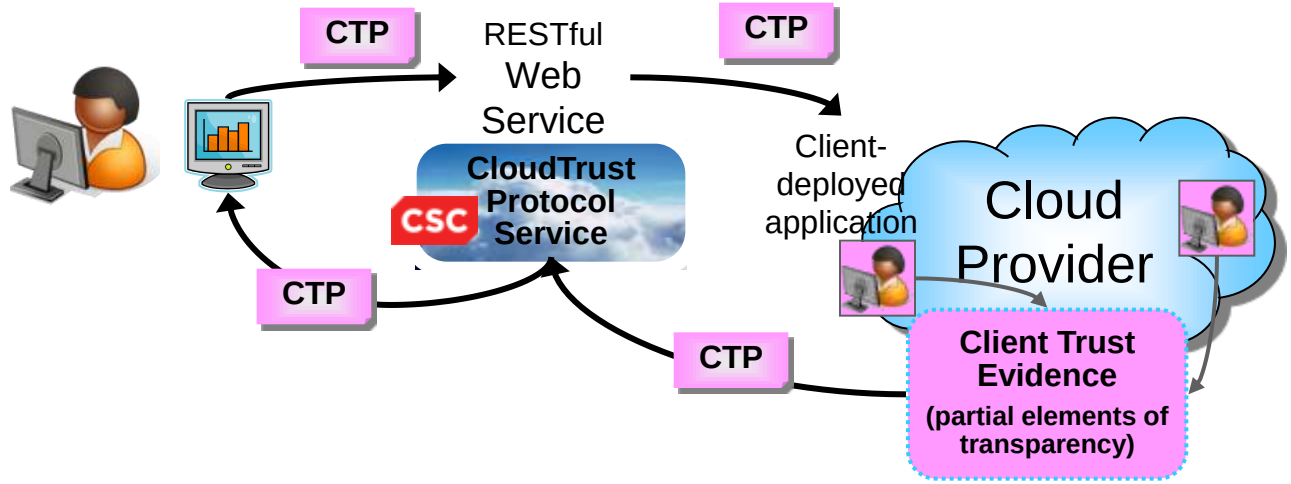


Scope of TaaS
Enterprise or Client-specific

- Enterprise

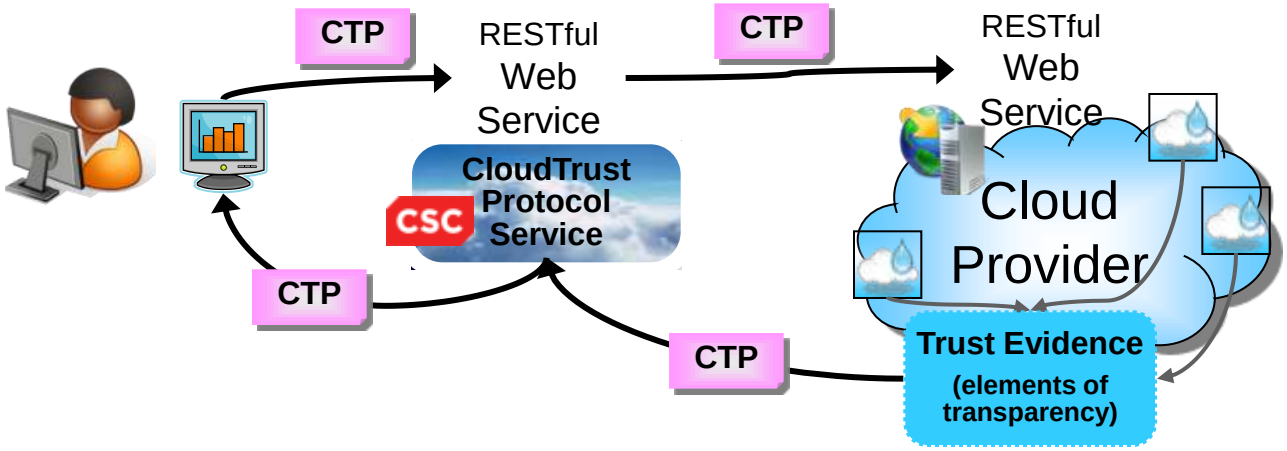


- Client-specific

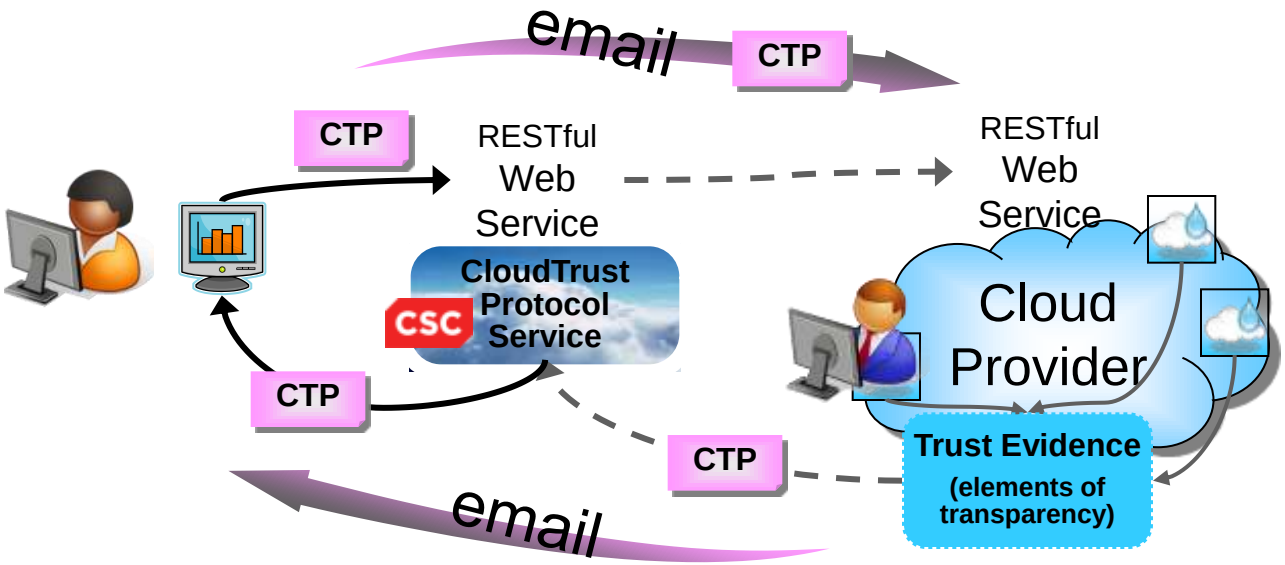


Multiple Styles of Implementation
The CTP is machine and human readable

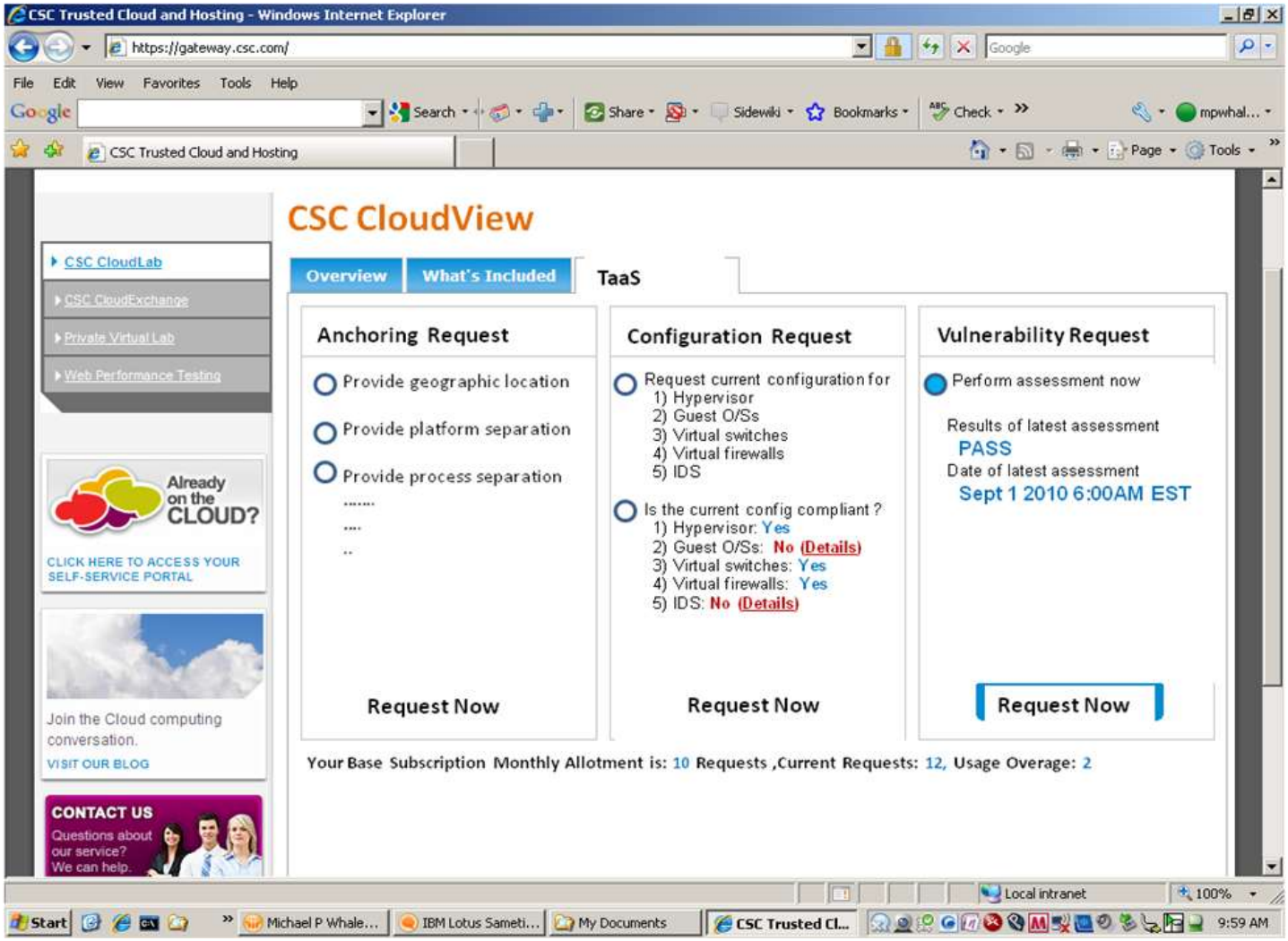
- In-band



- Out-of-band



For cloud consumers …

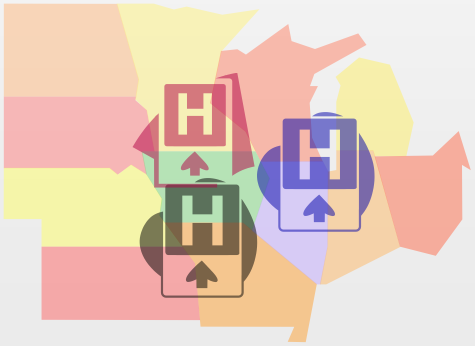


Imagine This!

Medical practice

18 GP's

2 Specialists



3 different hospitals and clinics in 2 different states

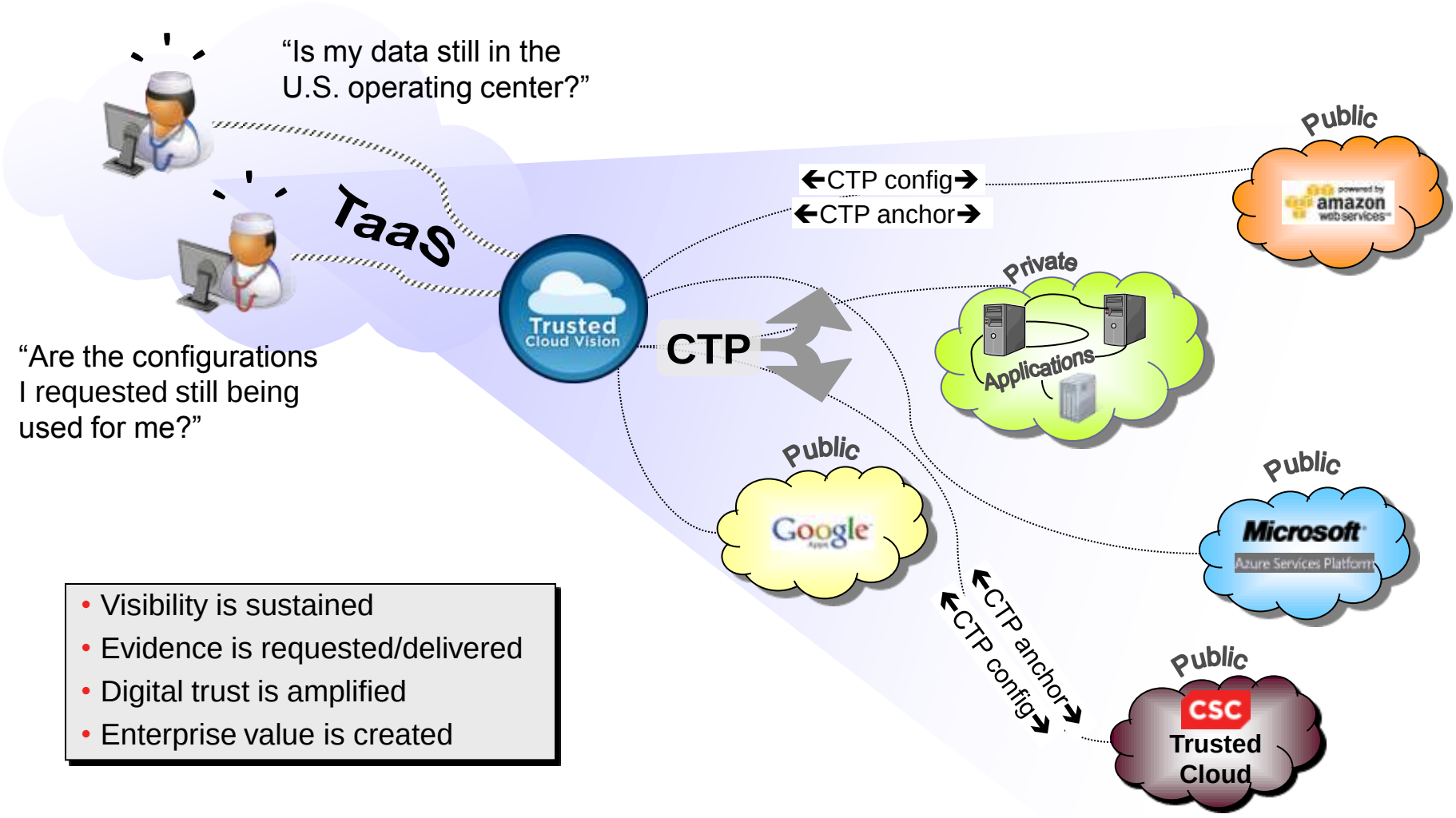
The Opportunity

- 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



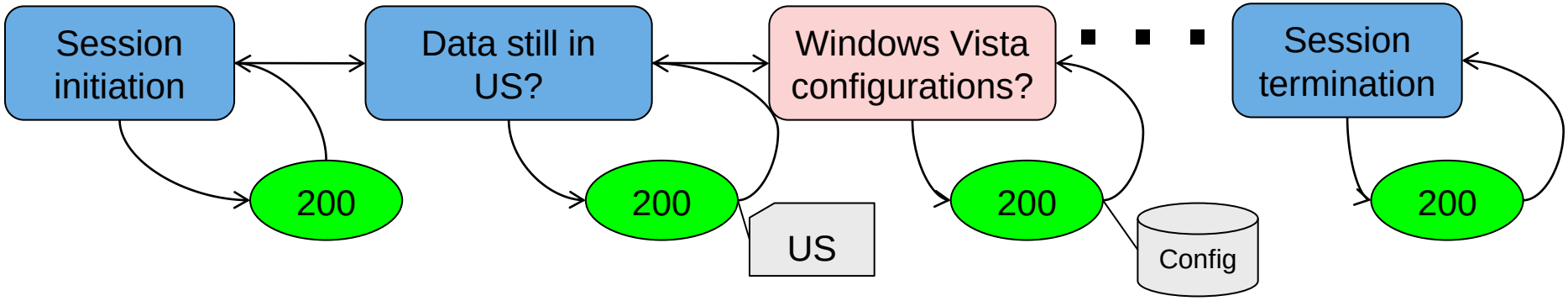
- Visibility is sustained
- Evidence is requested/delivered
- Digital trust is amplified
- Enterprise value is created

"… Right cloud. Right way."

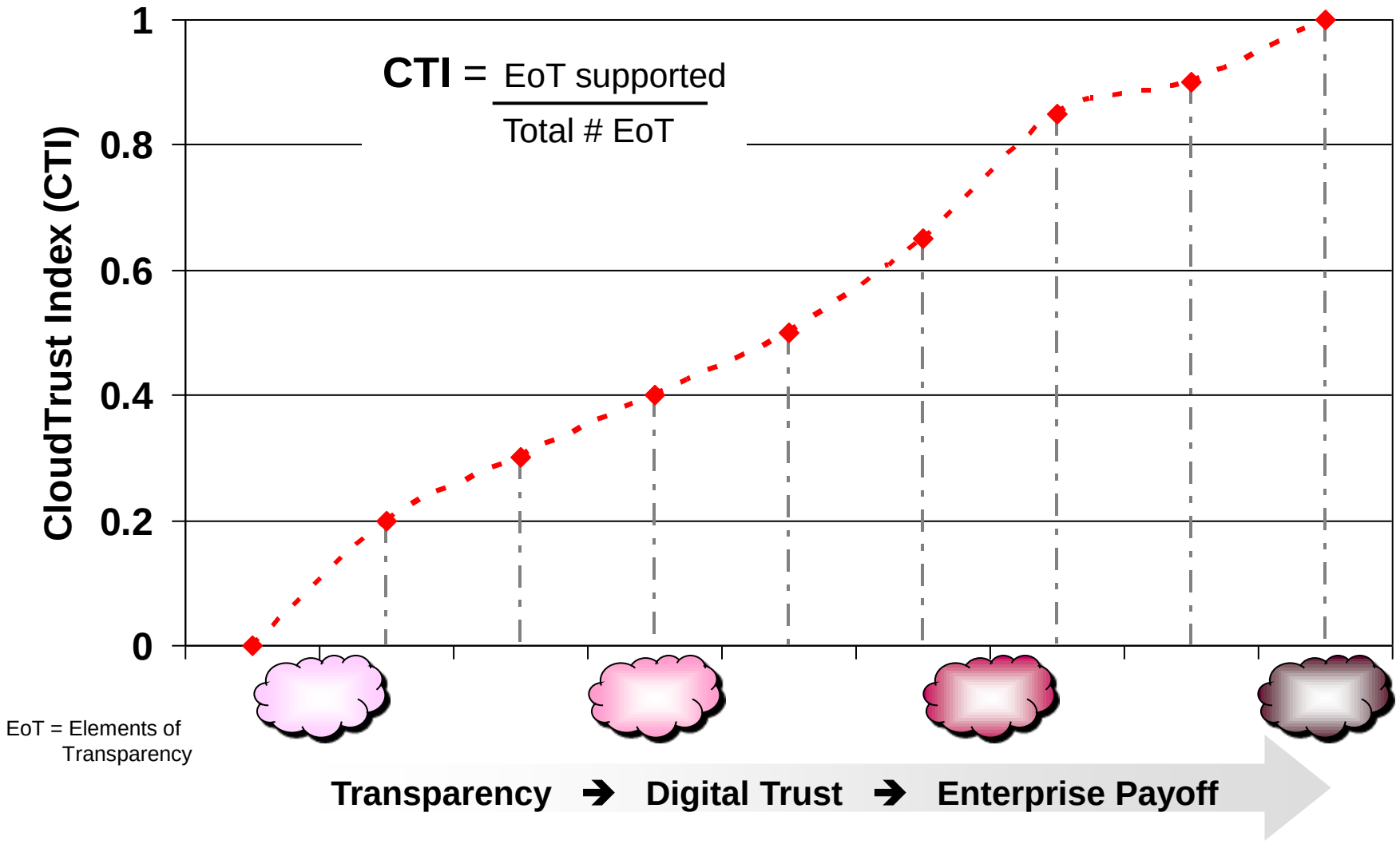
Request – Response, Asynchronous Operation

Appendix 1 of the Precis

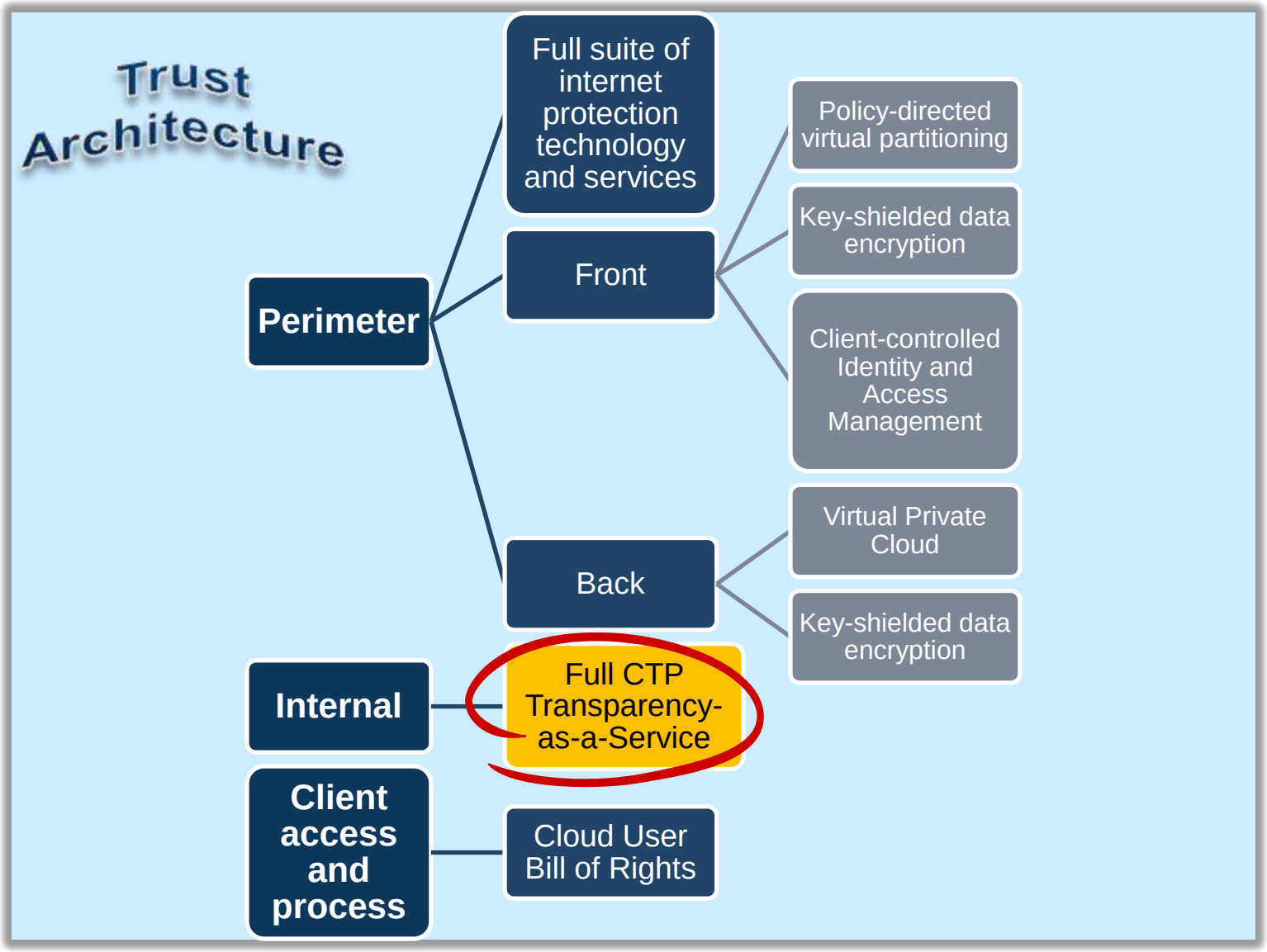
CTP Transaction Response Codes	
HTTP Response Code	**Meaning**
200	'OK' (with data) or 'YES'
204	Request received, but cloud vendor chooses not to respond
401	Unauthorized request
404	'NO'



The CloudTrust Index (CTI) as a Rough Measure of Transparency and Digital Trust Potential



The Trusted Cloud Services Trust Architecture
Digital Trust in the Cloud and From the Cloud



Clouds Come with Rainbows