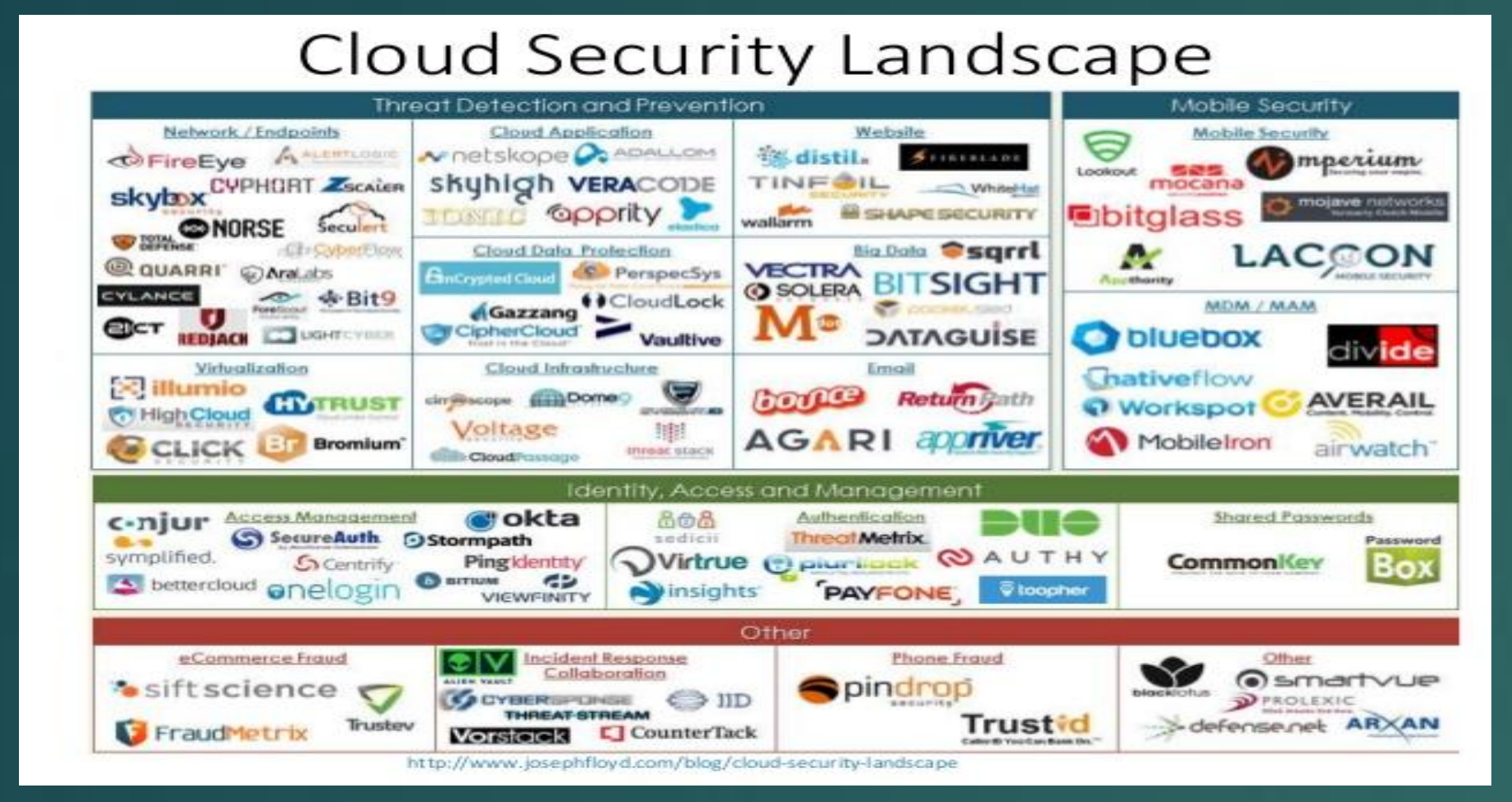
Towards a “Secure Cloud Model”

Student: Frank Lennon, Faculty Mentors: Dr. Soon Chun,
Information Systems & Informatics, 2800 Victory Blvd, Staten Island, NY 10314



Introduction

The Secure Cloud Model relates to the notion of “Cloud security framework” as a conceptual structure intended to serve as a support or guide for the creation of a secure information system. The intention of the proposed security framework is to serve as a comprehensive guideline for the creation, deployment, assessment and improvement of a Secure Cloud Model.

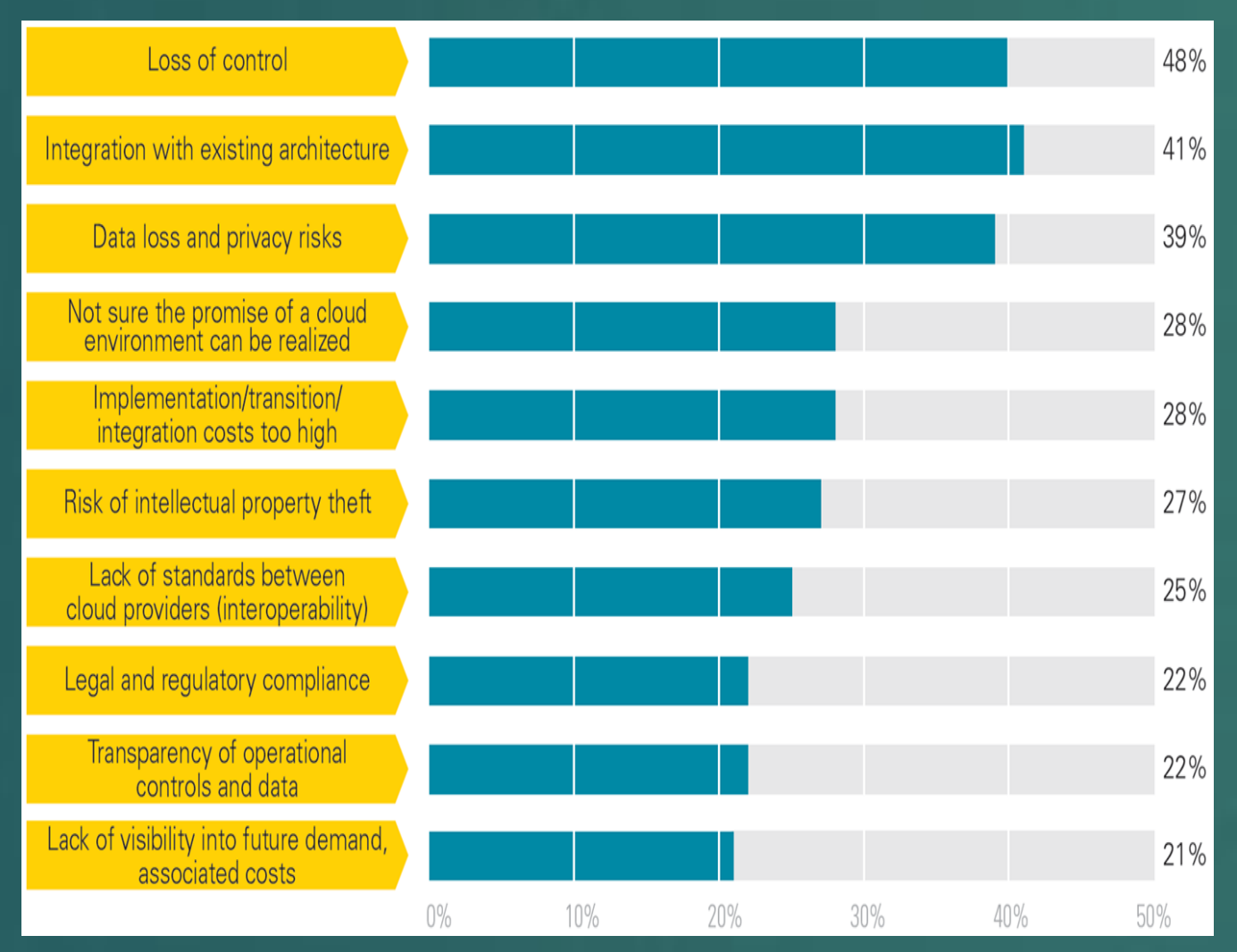
Enterprises recognize the value of cloud, research shows that 80% of organizations will be increasing their use of cloud services over the next two years. Employees want to use cloud services that are convenient, easy to use, and make their working lives simpler. However, business and employee views on cloud rarely correspond.

The outcome, often referred to as "shadow IT," is uncontrolled growth of cloud services, away from the watchful eyes of company IT departments.

When the company has given its blessing to a public cloud application, it still needs to enforce policies on the application regarding who can use it and whether data must be encrypted, etc.

Cloud Benefits and Problems

The advantages of adopting the cloud are clear, from the gains in end-user productivity to the efficiencies for IT staff, However , recent research shows that one in every three employees at Fortune 1000 organizations are uploading and sharing sensitive corporate data to third-party, cloud-based applications—and the employees know they are violating company/security policy.



Driving this use of “shadow IT” are

- better accessibility
- improved productivity and
- the convenience of cloud applications

Issues:

Security requirements are still stalling the broader adoption of cloud applications. \

One of the key challenges is that on-premises security products have a technology gap when it comes to cloud application usage and visibility.

Most products provide only partial protection—with limited capacity to see how and where cloud applications are actually being used. In addition, there is no easy way to enforce corporate policies for security and compliance.

Corporate Enterprises need to :

- control
- see
- monitor cloud application usage
- And protect against cloud-delivered threats, policy violations and risky user behavior.

Architecting the Cloud Application Security Model

With the strategic planning done, enterprises can follow their standard policies and practices to identify one or more appropriate solutions to evaluate that may suit their needs. Often, the alternatives revolve around suitability to task and ability to integrate with existing capabilities. The process can and should be iterative — many enterprises will already have piecemeal solutions in place to support small projects and proof-of-concept use cases.

At a broader procedural level, the enterprise should follow these steps:

- ❑ Identify the users, data, and applications within the scope of the project
- ❑ Map how the users, data, and applications interact with each other
- ❑ Instrument the paths among the elements with a solution for monitoring and policy enforcement
- ❑ Employ a solution that consolidates security management functions from disparate cloud applications into a single management console

Assessing Existing Security Solutions

Large enterprises already have huge investments in their security architecture. In the move to the cloud, they must determine which solutions are likely to provide some benefit and which will not. In addition, as architecture and models are assessed, a similar set of capabilities must be built out that are tailored to address cloud applications.

Some of the common solutions with capabilities that must be ported to the cloud are:

- ❑ **Secure Web gateways** can capture and assess the requests from endpoints to determine whether access is allowed. Having pioneered this capability with inappropriate Web sites, the solutions often provide information useful for a more thorough review of cloud application usage.
- ❑ **Identity management solutions** provide mature processes to provision, monitor, and deprovision users and accounts across many applications inside the datacenter. As cloud applications become more prominent, the need to provide a similar capability for the new applications increases in importance as well.
- ❑ **Threat management solutions** provide intrusion detection/prevention and security event management capabilities for identifying attacks against an organization's resources.
- ❑ **Mobile device management solutions** provide management capabilities for provisioning and deprovisioning mobile devices. Mobile-to-cloud connectivity creates a new path for security solutions to address.

Each of the solutions should be evaluated for their ability to address cloud applications. Some will likely be deficient in their visibility, for example, or their ability to integrate with cloud solutions.

Cloud Trust Protocol (CTP)

The Cloud Trust Protocol (CTP) is designed to be a mechanism by which cloud service customers can ask for and receive information related to the security of the services they use in the cloud, promoting transparency and trust.

Why CTP?
The creation of CTP was motivated by the current gaps in cloud security monitoring. Though many cloud providers offer solutions such as dashboards or ad-hoc APIs in order to enable cloud customers to monitor cloud services, these solutions have some strong shortcomings when it comes to the security of cloud services.

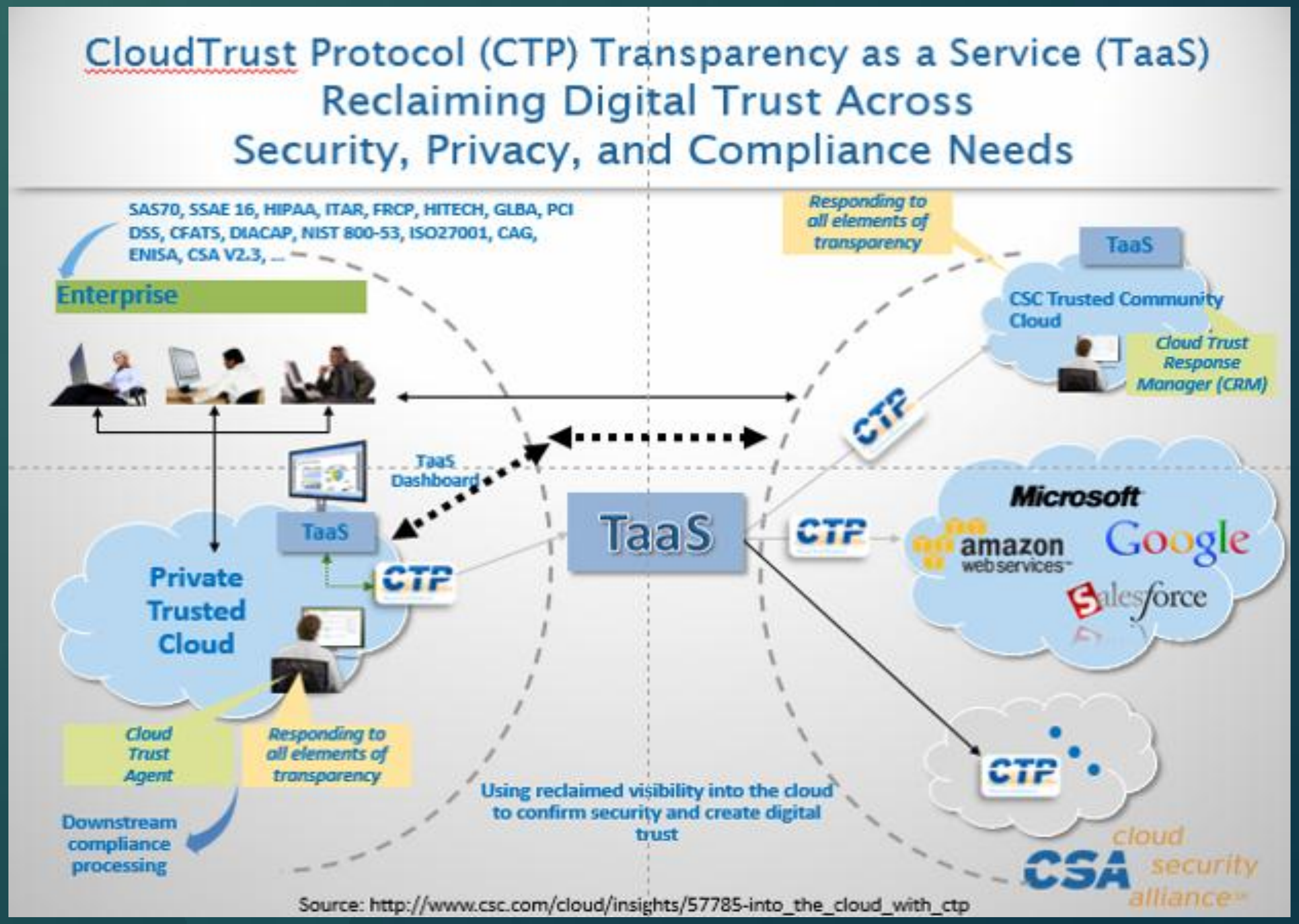
1. the solution is usually proprietary and not interoperable.
2. they often target performance indicators rather than security.
3. the measurements conducted by providers are often imprecisely described in terms of parameters and scope.
4. each provider typically uses subtlety different metrics for similar attributes, making any comparison with a customer-defined baseline challenging while making the ranking of competing services near impossible.

The API aims to solve
the first and third issues, while creating a platform tailored to support a solution to the other two remaining issues, which will require further standardization initiatives by relevant stakeholder(s).

The CTP Data Model and Application Programing Interface (API), including:
• The format of CTP messages exchanged between cloud service customers and providers.
• The modeling of concepts such as “security attributes”, “objectives”, “measurement results” and “triggers” in machine readable format.
• The means to define the scope of the service to which CTP monitoring queries apply.

However, a specification of the “security attributes” (and associated metrics) that are queried by CTP.
will need to be provided by the Cloud Security Alliance and will likely be influenced by upcoming standards such as [ISO_19086]. CTP also offers implementers the choice to define and adopt their own set of security attributes and related metrics.

Cloud Trust Protocol TAAS


CloudTrust Protocol (CTP) Transparency as a Service (TaaS)
Reclaiming Digital Trust Across
Security, Privacy, and Compliance Needs
SAS70, SSAE 16, HIPAA, ITAR, FRCP, HITECH, GLBA, PCI DSS, CFATS, DIACAP, NIST 800-53, ISO27001, CAG, ENISA, CSA V2.3, ...
Enterprise
Responding to all elements of transparency
TaaS
CSC Trusted Community Cloud
Cloud Trust Response Manager (CRM)
CTP
TaaS Dashboard
TaaS
TaaS
CTP
Private Trusted Cloud
CTP
Microsoft
amazon web services
Google
Salesforce
Cloud Trust Agent
Responding to all elements of transparency
Downstream compliance processing
Using reclaimed visibility into the cloud to confirm security and create digital trust
CTP
cloud security alliance
CSA

Source: http://www.csc.com/cloud/insights/57785-into_the_cloud_with_ctp