CURRENT CHALLENGES AND FUTURE DIRECTIONS FOR CLOUD SECURITY

Jim Reavis
CEO, Cloud Security Alliance

State of Cloud

Cloud is now the leading IT system on a global basis

- Cloud infrastructure spending exceeded traditional IT in 2018 for the first time (Source IDC)
- ”Cloud First” strategy for new IT projects
- Industry leaders tend to be cloud leaders
- Agility, Cost, Developer mindshare, Tier 1 cloud providers more secure than nearly all on-premise alternatives

Cloud is mature – CSA is 10 years old!

- Certificate of Cloud Security Knowledge (CCSK, personal certification) – 9 years old, Body of Knowledge updated 4 times
- Cloud Controls Matrix (CCM, control objective framework) – 8 years old, most widely downloaded CSA research
- CSA Security, Trust and Assurance Registry (STAR, provider certification) – 7 years old, approx 600 entries

CCSK™
Certificate of
Cloud Security Knowledge

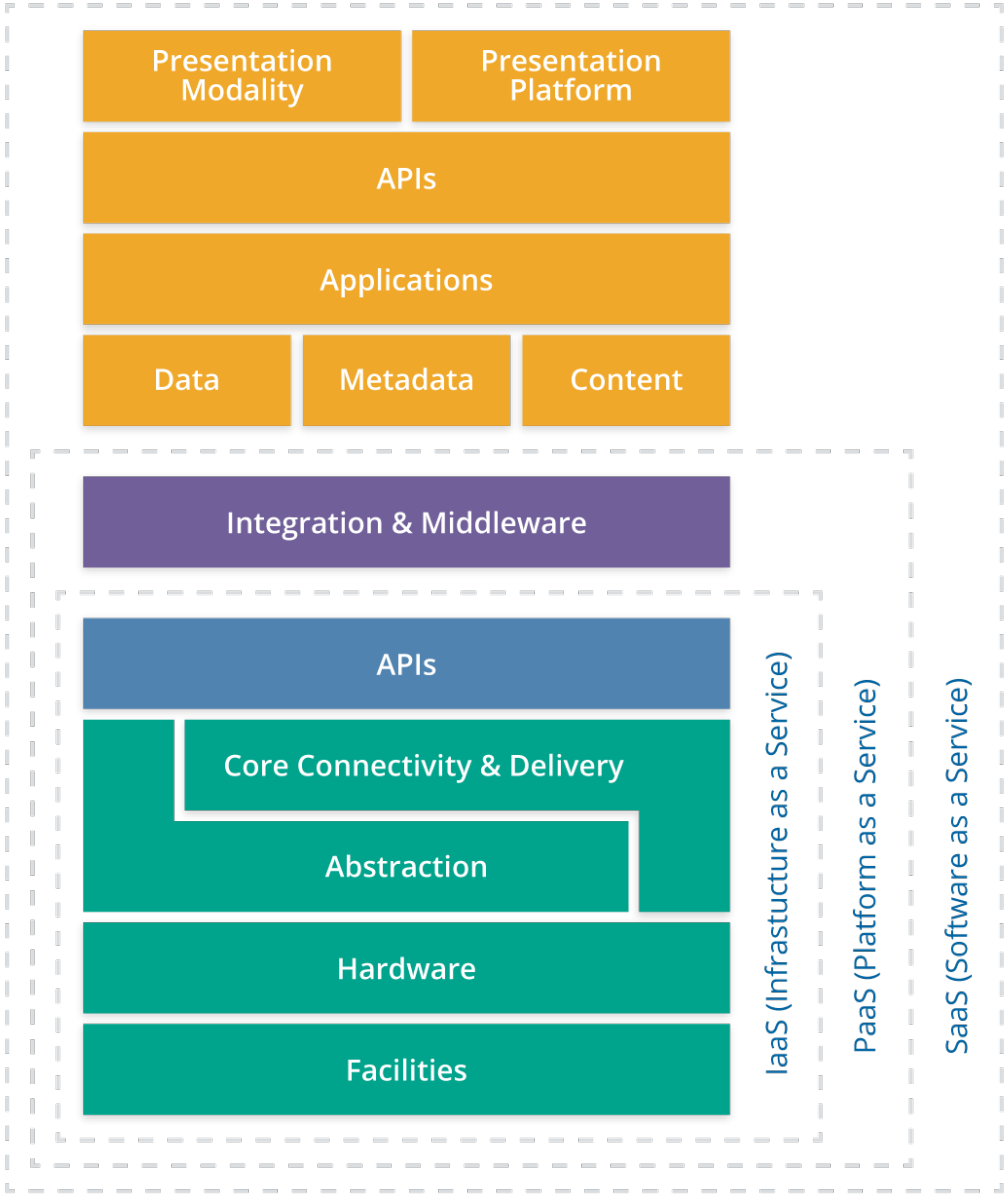
CCM™
Cloud Controls Matrix

CSA STAR™
Security, Trust & Assurance
Registry

CSA cloud security alliance®

The Cloud Security Focus

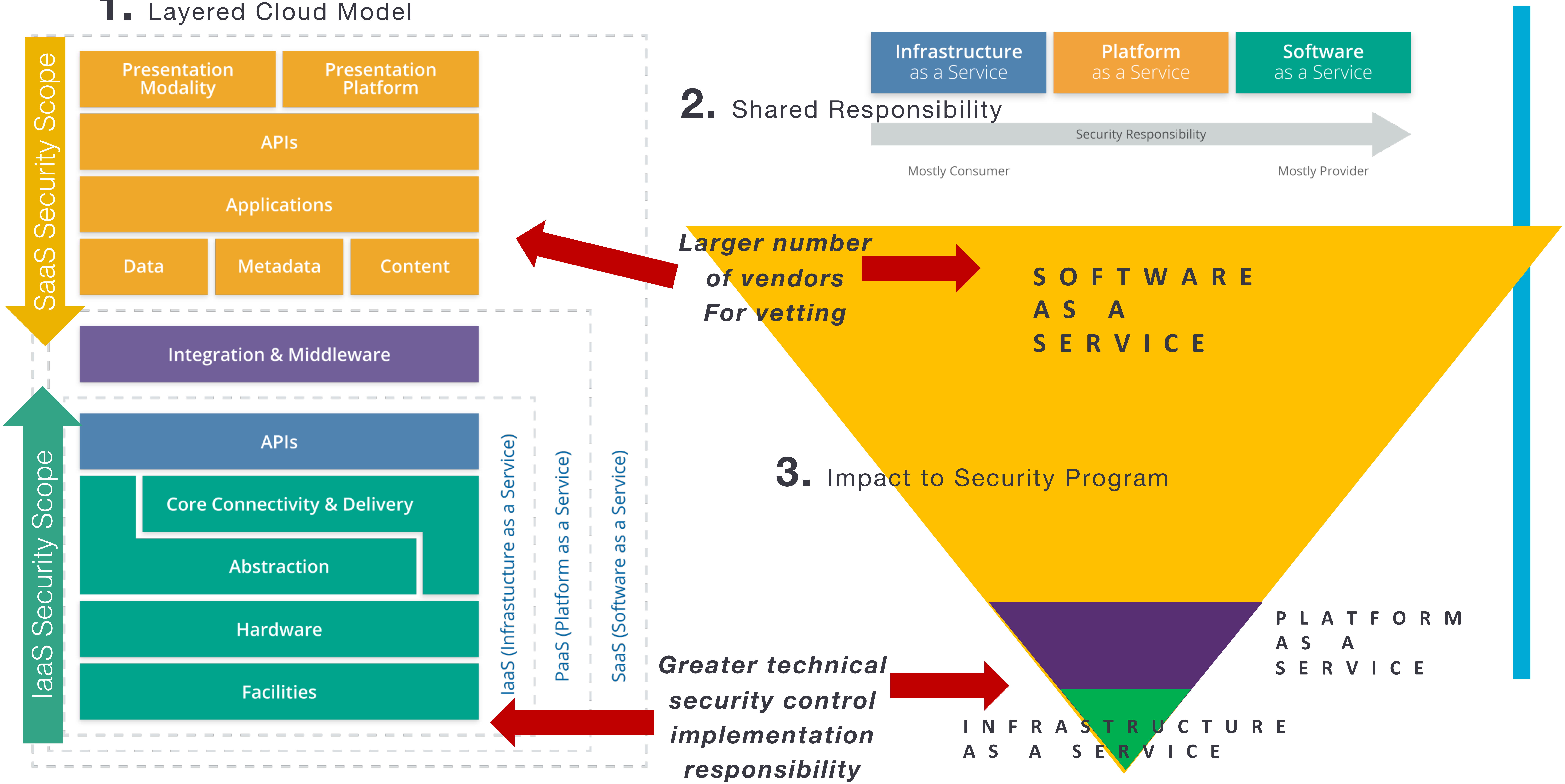
Cloud Reference Architecture



CSA Cloud Reference Model - 2009

- Cloud as a layered model
  - SaaS has implicit IaaS & PaaS layers
  - Businesses occupy individual layers
- Framework theory similar to OSI networking model
- Allows rationalizing the “Mashup” nature of virtually all cloud applications
- Data centers are Virtual, a “Software Construct”
- Code is continuously updated
- SaaS should “inherit” the controls and compliance of the lower layers
- Assurance activities should avoid redundancies
- Assurance activities will need to be more frequent to reflect dynamic nature of cloud

Understand the Cloud Security Focus



1. Layered Cloud Model

SaaS Security Scope

Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

Integration & Middleware

IaaS Security Scope

APIs

Core Connectivity & Delivery

Abstraction

Hardware

Facilities

IaaS (Infrastucture as a Service)

PaaS (Platform as a Service)

SaaS (Software as a Service)

2. Shared Responsibility

Infrastructure as a Service

Platform as a Service

Software as a Service

Security Responsibility

Mostly Consumer

Mostly Provider

3. Impact to Security Program

Larger number of vendors For vetting

SOFTWARE AS A SERVICE

PLATFORM AS A SERVICE

INFRASTRUCTURE AS A SERVICE

Greater technical security control implementation responsibility

Enterprise Concerns?

- Cloud attacks & breaches will explode, probably based on basic threats
- What are the Wild Cards?
  - Total Cloud Meltdown? Not seen as likely, any more than the Internet
  - “Snowden” events leading to widespread lack of trust in the model and players? More likely

- Security at Scale
  - Ubiquity of compute (cloud & IoT), storage (cloud & IoT) and bandwidth (5G)
- Pervasive compute (Cloud, Big Data, IoT, 5G, etc) leading to a Loss of Privacy?
  - GDPR is not the last privacy regulation, more will come – with stricter requirements
  - In the future, will you be allowed to have databases of PII if you cannot provide security?
- Can we retool and grow a cloud security workforce?
- Let’s not forget the business, can we keep pace with digital transformation?

The Multi-Cloud Question(s)

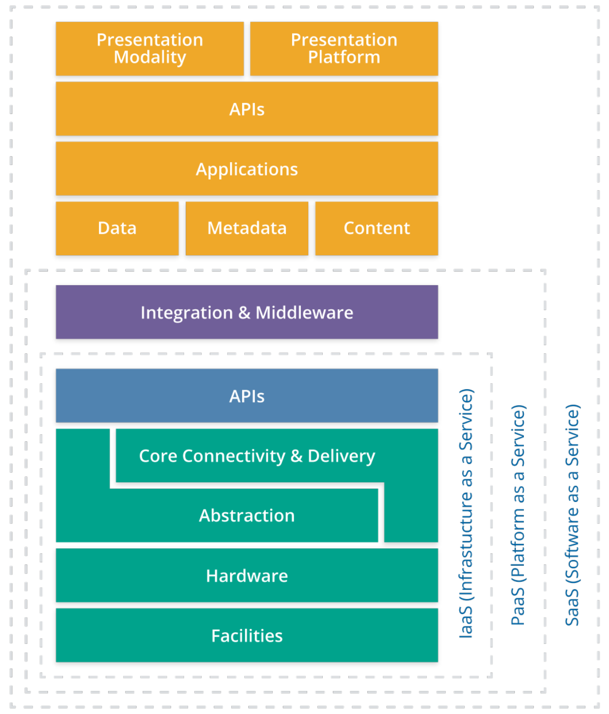
- All organizations are multi-cloud, the question is to which degree?
    - At least 1 IaaS CSP, often more
    - On-premise IT, private cloud
    - Many SaaS CSPs
- Are security policies uniformly applied?
- Are organizations able to move workloads between clouds?
- Are organizations able to migrate to competing clouds?
- Does multi-cloud enable agility & innovation?
- Are risks reduced or increased in multi-cloud?

Enterprise Directions

- Moving from information security to cybersecurity
- Cybersecurity skills gap remediation
- Scale & Automation
  - DevOps/DevSecOps
  - Machine Learning
- Highly virtualized, API-driven models
  - Zero Trust
  - Microsegmentation
  - Software Defined Everything
  - Containerized, Microservices & Serverless
  - Structured frameworks and orchestration to shrink threat windows
  - Highly dependent upon identity and crypto advances
- Blockchain = Worldwide ledger of trust

Multi-Cloud specific strategies

- DevOps & Containerization = create levels of abstractions over different clouds
- CSA Cloud Controls Matrix = achieve uniformity in security control objectives in very different cloud environments
  - CSP, Tenant & cloud layer responsibility
  - Can use CSA STAR to assist: www.cloudsecurityalliance.org/star
- Robust Identity Management strategy
  - Identity federation with all clouds
  - Strong authentication
- Push for 100% cloud visibility
  - Cloud Access Security Broker or similar
  - Logfile management & Cloud SOC



CSA STAR™
Security, Trust & Assurance Registry

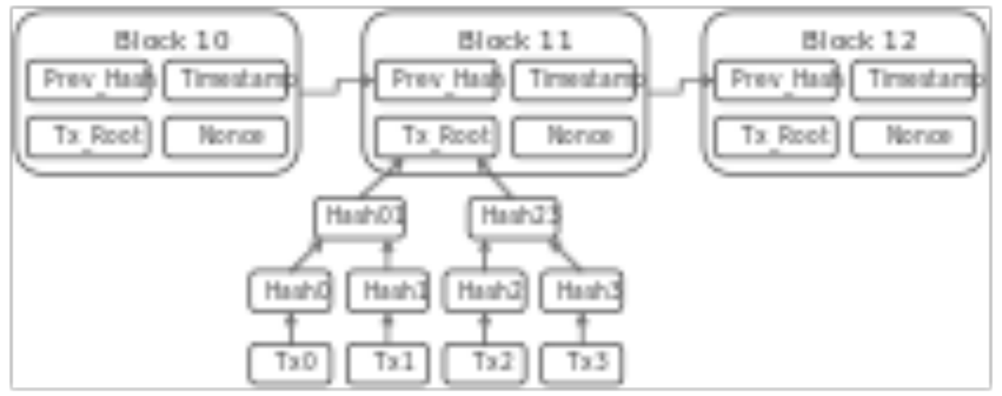
CCM™
Cloud Controls Matrix

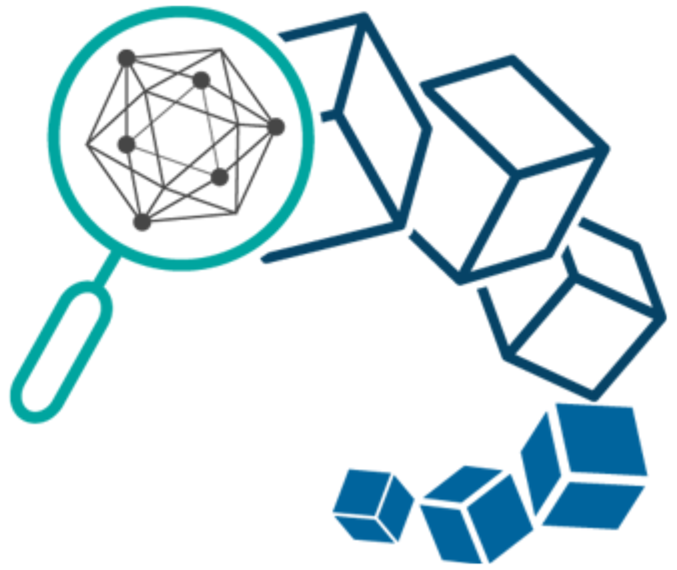
Blockchain as a Security Game Changer?

1993
"On the Internet, nobody knows you're a dog."

2015
NSA
We know

Blockchain



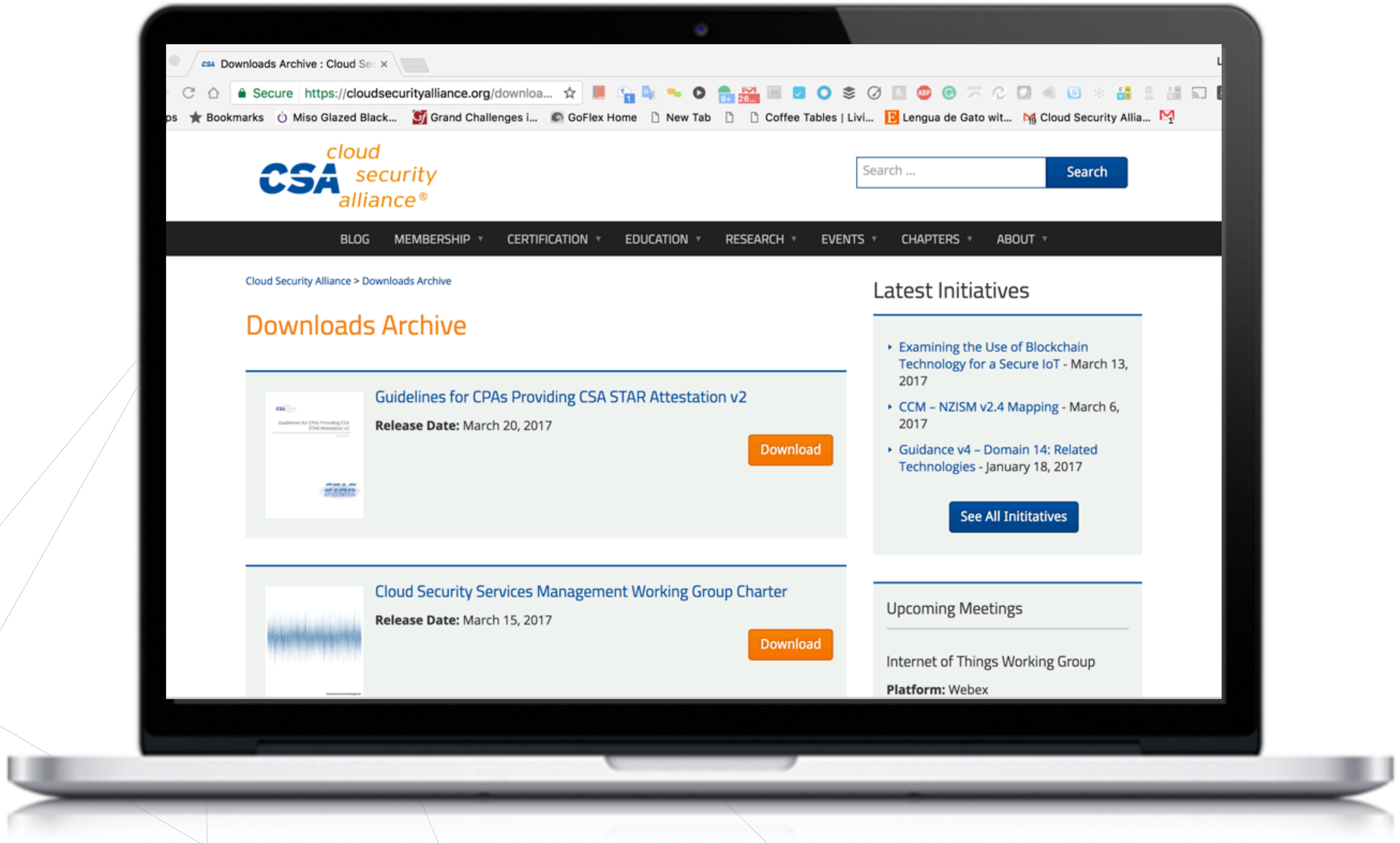


- Blockchain: the immutable logging infrastructure at the heart of cryptocurrencies
- Blockchain being applied to many other solutions: supply chain, non-financial transactions
- Rapid improvements introduced
- Wide variety of implementations: Permissioned vs permissionless, Consensus models, Chaining, Forking
- NIST description: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf
- Not a silver bullet, but we feel it will reshape the Internet and Cloud in profound ways

Cybersecurity at the Intersection of Cloud & Blockchain

- Cloud + Blockchain + Community (people)
- Performance, scale, automation and agility of Cloud
- Privacy, immutability and security of Blockchain
- ***Blockchain provides a security, transparency, accountability layer on top of cloud, and puts it in the hands of the users***
- We need to marry Cloud + Blockchain and reinvent applications and disrupt cybersecurity
- CSA is taking this big picture approach and applying it to targeted opportunities within cybersecurity and privacy
- We think there will be a few standard public Blockchains the cybersecurity industry will agree on using

Thank You!



Cloud Security Alliance > Downloads Archive

Downloads Archive

Guidelines for CPAs Providing CSA STAR Attestation v2

Release Date: March 20, 2017

Cloud Security Services Management Working Group Charter

Release Date: March 15, 2017

Latest Initiatives

- Examining the Use of Blockchain Technology for a Secure IoT - March 13, 2017
- CCM – NZISM v2.4 Mapping - March 6, 2017
- Guidance v4 – Domain 14: Related Technologies - January 18, 2017

Upcoming Meetings

Internet of Things Working Group

Platform: Webex

Contact CSA

Email: info@cloudsecurityalliance.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org