RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: CDS-R03

Security Lessons Learned: Enterprise Adoption of Cloud Computing

Jim Reavis

Chief Executive Officer
Cloud Security Alliance
@cloudsa

#RSAC

Agenda

- What we are going to cover
  - The current & future state of cloud computing adoption
  - Security best practices learned by enterprise users of cloud
  - The security perspective of the cloud providers
  - Cloud security trends changing the market
  - How to apply the lessons learned to your own cloud computing security strategy

Cloud in the Enterprise 2015

- Awareness: Capturing data on current cloud usage within organization
- Opportunistic: Identifying strong cloud adoption opportunities
- Strategic: Building cloud adoption program - architecture, frameworks & business alignment

- Data security is a board level issue in over 60% of enterprises (CSA/SkyHigh Networks survey 2015)
- Leveraging hybrid clouds: public and private
- Supporting multiple assurance requirements

What are leading edge organizations doing?

- Implementing cloud security intermediaries such as CASB: Cloud Access Security Broker
- Applying security to DevOps and DevOps to security
- Container technologies: Docker, Rocket
- Security analytics
- Integration of Internet of Things
- Creating new native cloud security strategies

Cloud of the Future

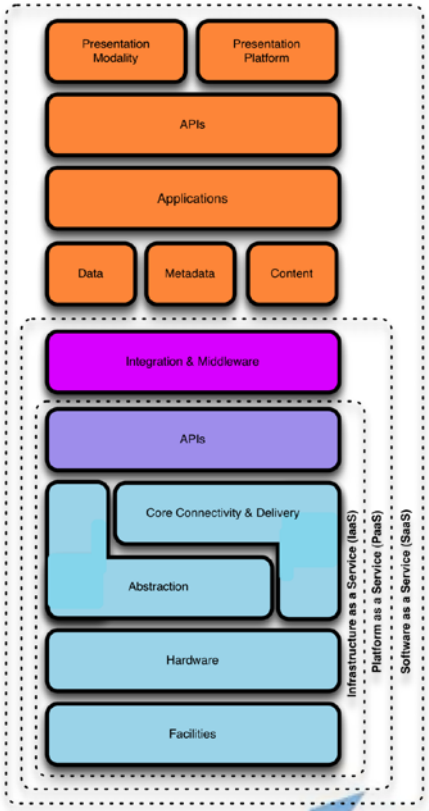
- Cloud 2020
  - Leading edge enterprises will be all cloud (and more successful)
  - Mainstream enterprises will be majority cloud (Cloud First)
  - Majority of endpoints will be outside corporate control (e.g. BYOD, Cloud Managed)
  - Majority of cloud connected devices are Internet of Things
  - Vendor-neutral Virtual Private Clouds compete with Private Clouds
- Mastering cloud security by 2020 requires advancement in people, process and technology
- Understand the power – ***One line of code can create a datacenter!***

Cloud Lessons

- Misunderstanding different types of Clouds and your Role
- Unrealistic expectations of customized services from providers
- Forcing legacy tools & architectures on cloud security problems
- Heavy-handed blocking of cloud services backfires on infosec
- Using compliance as a pretext for inaction
- Key role of intermediaries

Different types of clouds

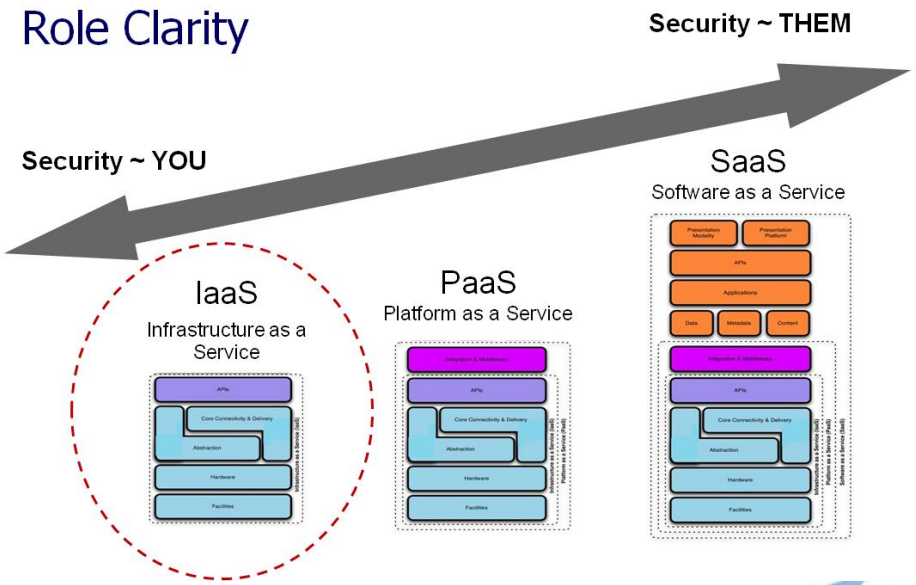
- Cloud as a layered model (eg OSI)
  - SaaS has implicit IaaS layers
- Market impacts architecture
  - Businesses occupy individual layers (e.g. cloud brokers)
  - Layers of abstraction emerge
  - Innovation/optimization in layers
- Everything becomes virtualized



CSA Cloud Reference Model

Customer role in different clouds

- In all clouds it is a shared responsibility
- IaaS is a greater responsibility for the customer to harden the service
- Provider is responsible for implementing security in SaaS
- Customer has the ultimate responsibility for security assurance



Why isn't my cloud experience customized?

- Managing a standardized environment is simpler, lowers costs and increases availability
- Software feature requests must be desired by a large percentage of the customer base
- Physical datacenter audits are rare (and usually pointless when possible)
- Customer doesn't get complete access to full technology stack
- Highly customized systems carry high TCO

The legacy security problem

- Security professionals bring an existing mindset to cloud security
  - AV, IDS, Patch management, Forensics must be done differently in cloud
- Traditional datacenters are relatively static
  - Clouds change constantly
- Network security solutions assume an appliance access to traffic
  - Cloud traffic traverses hypervisors, SDN
- Security operations centers (SOCs) assume ability to instrument IT systems
  - Cloud solutions may not have an agent or logfile access for your SIEM

Compliance

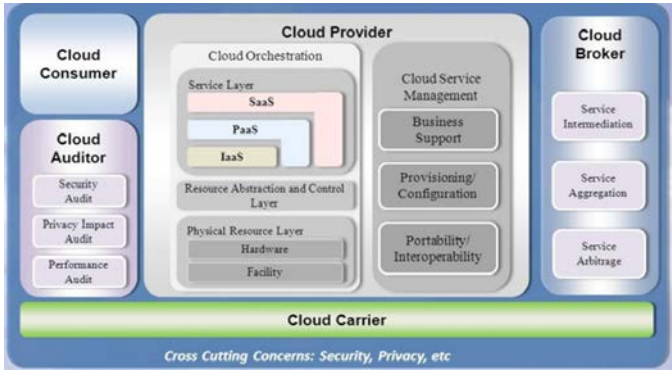
- Regulations and standards are almost all “pre-Cloud”
- Many regulations assume customer controls full technology stack
- Many industries & gov’ts want “in-country” data processing
- Virtually all regulations have flexibility to allow for reasonable interpretation to address “spirit of law”
- Demonstrating compliance in cloud to auditors is another “shared responsibility” between customers and providers

The provider perspective

- Huge variety in the types of cloud providers, their security credentials and ability to execute on a security strategy
- Good providers understand good security is a matter of corporate “life or death”
- Good providers invest far more in security than an enterprise
- Providers feel redundant compliance and customer audit requirements is detrimental to their security efforts
- Providers often reluctant to embrace transparency about their security practices

Key role of intermediaries

- Cloud providers too diverse to hope for uniform security capabilities
- Enterprises lack resources to drive requirements into provider environments
- Enterprises in a transitional phase in security strategy, architecture and tools to meet the cloud challenge
- Intermediaries
  - Reduce multi-cloud complexity from a customer point of view
  - Create layers of abstraction
  - Provide security augmentation to native cloud feature sets

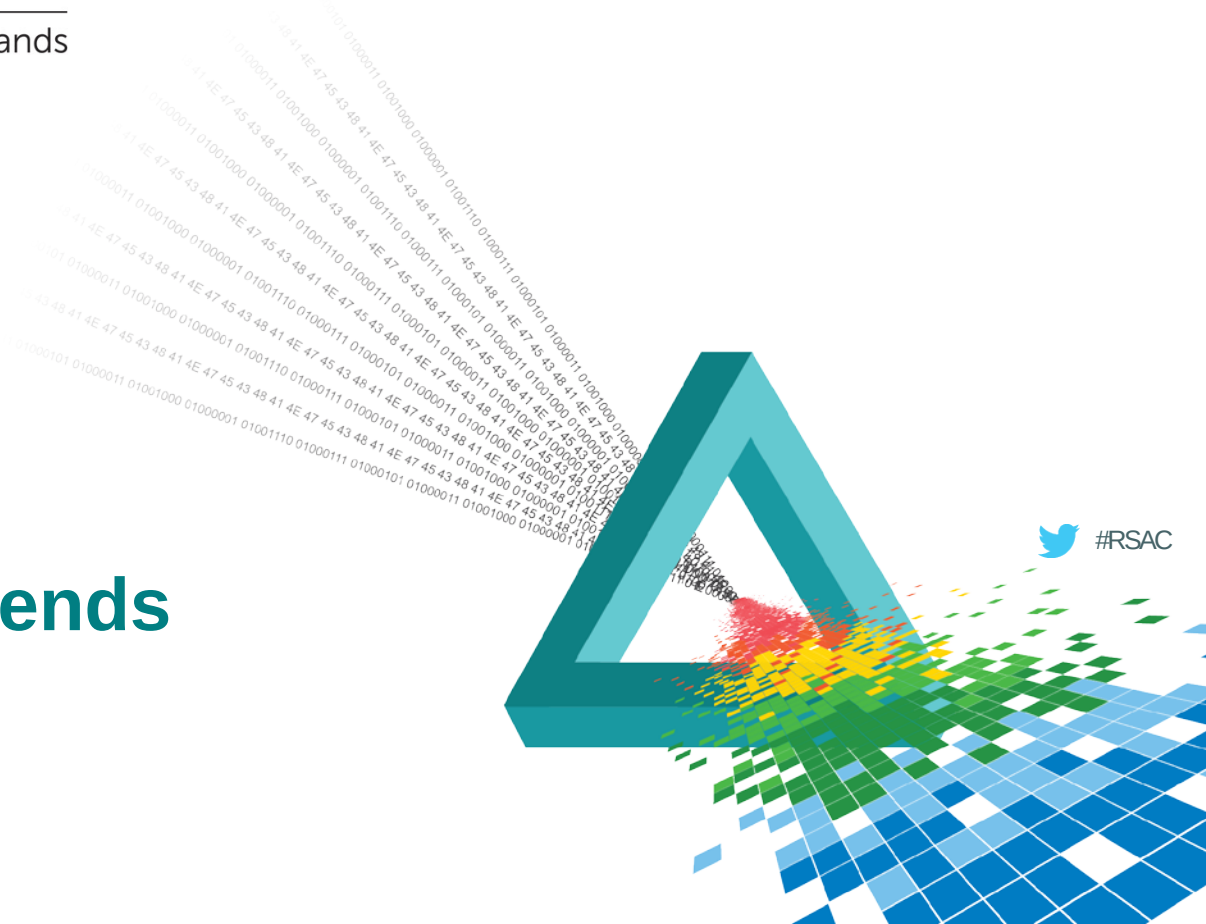


Source: NIST

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Cloud Security Trends



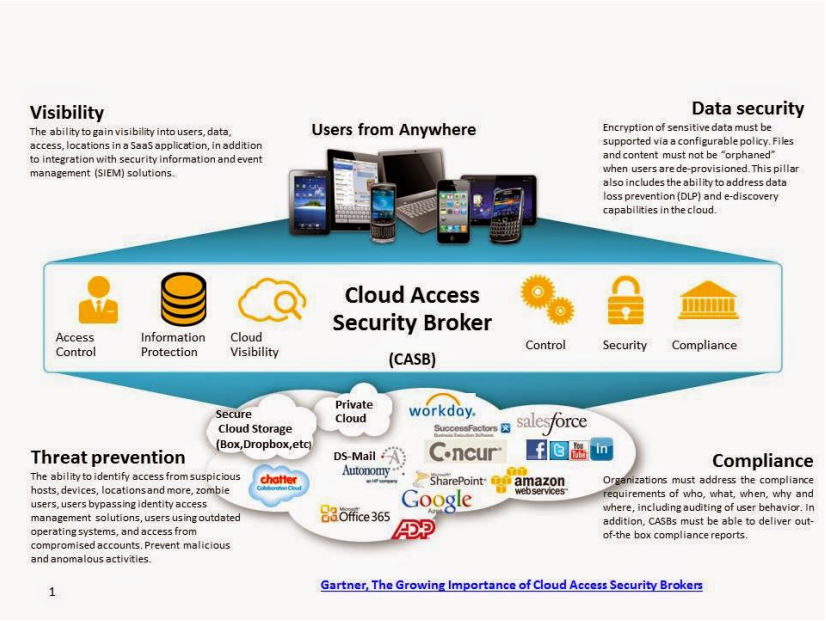
#RSAC

CASB: Cloud Access Security Broker

- Gartner: Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.

CASB: Cloud Access Security Broker

- Varied deployments
  - Perimeter
  - Reverse Proxy
  - Cloud Provider API integration
- Functions
  - Decision support
  - Context-based policy enforcement
  - Opportunistic encryption
  - Identity federation
- Needs
  - Standards for providers and customers to interface and integrate
  - Common policy language, compliance and risk metrics



Unique native cloud features benefitting security

- Disposable Infrastructure
- Dynamic scaling of “physical” resources
- “Unlimited” provisionable bandwidth
- Per-resource security controls
- On-demand virtual datacenters
- Real-time stream processing
- Unlimited storage (both blob and warehoused)
- Programmatic Key Management
- DDoS Avoidance (elasticity)
- …and more!

Thinking Virtually…

Awesome list courtesy of Tim Prendergast
www.evident.io

Understanding how to leverage cloud to do security better

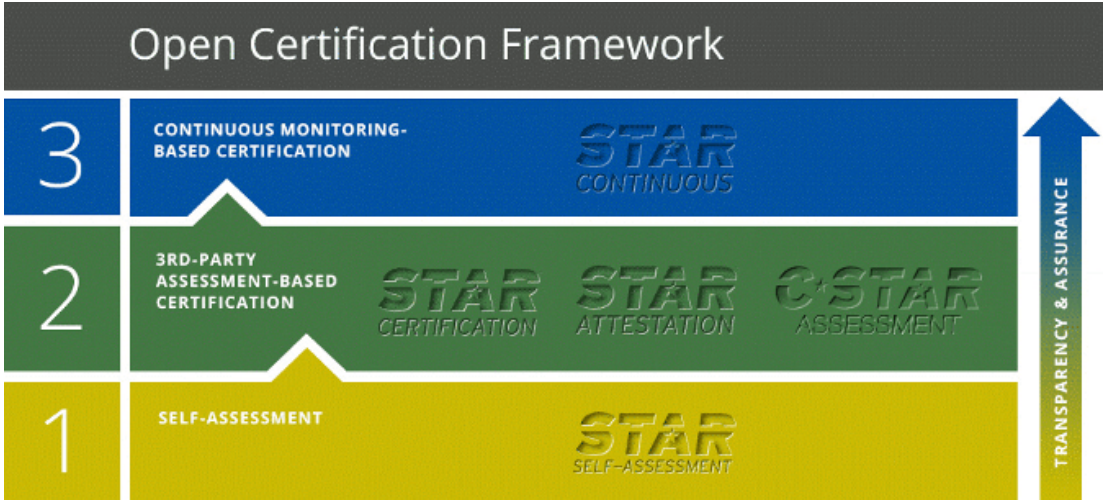
- Scale out over DDoS Attacks rather than block them
- Destroy compromised servers, retaining image for later forensics
- High-risk operations can be containerized and single-use
- Programmatic changes in response to attack patterns/behaviors
- Short-lived resources have minimal impact when compromised
- API-centric services are not vulnerable to traditional network attacks
- Think about security as DevSecOps

Awesome list courtesy of Tim Prendergast www.evident.io

Making cloud providers accountable: CSA Security, Trust and Assurance Registry (STAR)

- Based upon Cloud Controls Matrix meta-framework
- World's largest cloud assurance registry

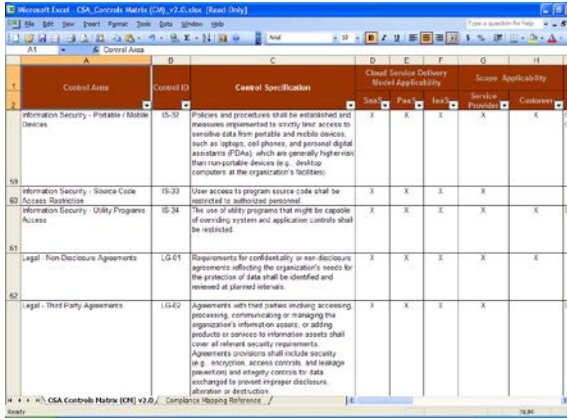
CCM™
Cloud Controls Matrix



Cloud Controls Matrix – backbone of STAR

CCM™
Cloud Controls Matrix

- Controls derived from CSA guidance organized into a meta-framework of 16 domains
- Foundation for all cloud assurance programs
- Mapped to familiar frameworks: ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP – mappings growing virally
- Rated as applicable to S-P-I
- Customer vs Provider role
- CAIQ – Questionnaire format



	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability	
1				SaaS	PaaS	IaaS	Service Provider	Customer
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X	
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X
62	Legal - Non Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X
	Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X	

CAI™

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Applying the knowledge to your enterprise

#RSAC

Apply the knowledge (1/3) – baseline & foundation

- Use egress monitoring, CASB or similar to gain visibility and build a report of your cloud usage
- Survey your staff's cloud experience
  - Hands on experience with at least 2 IaaS, at least 1 PaaS and Security as a Service?
  - Do you have any CCSKs on staff (Certificate of Cloud Security Knowledge)?
- Build your cloud security framework
  - Cloud Controls Matrix (CCM) is a good start
  - Assign a team member to map CCM to your own Information Security Management System (ISMS)

Apply the knowledge (2/3) – gentle policing of cloud usage

- Gain visibility into the use and risk of cloud services
- Educate employees to use low risk services leveraging existing infrastructure
- Integrate anomaly detection with SOC for investigation and remediation
- Identify sensitive data stored in sanctioned services (e.g. Box, Salesforce, Office365)
- Secure data in sanctioned services with encryption, DLP and access control policies
- Encourage/require providers to list in CSA STAR or minimally fill out CCM/CAIQ for you

Awesome list courtesy of Jim Routh, Aetna and SkyHigh Networks

Apply the knowledge (3/3) – build your future cloud strategy

#RSAC

- Educate security team that cloud requires greater agility
  - Shorter risk assessment cycles, constant state of change is the new norm
  - Identify bottleneck processes that don't scale to cloud speeds and fix them
- Build new, cloud-native security strategies
  - New approaches for anti-DDoS, forensics, patch mgt, malware, etc.
  - Identity federation dialtone
  - Audit security architecture for physical dependencies
  - Leverage Security as a Service to secure *aaS
- Research new technologies before business adopts, e.g. containers
- Demand transparency from the cloud provider industry

Security at the speed of cloud is scary – and necessary

- Culture change ahead
- But, the real security “Achilles Heel” for enterprises is legacy IT

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: CDS-R03

THANK YOU!
Security Lessons Learned: Enterprise Adoption of Cloud Computing

Jim Reavis

Chief Executive Officer
Cloud Security Alliance
@cloudsa

#RSAC