RSA Conference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: CMI1-R03

State of Cloud Security 2016

Jim Reavis

CEO

Cloud Security Alliance

@cloudsa

#RSAC

Agenda

- What we are going to cover
  - Market forces pushing us into the cloud
  - The latest thinking on cloud computing security threats
  - Perspective of enterprise users on the state of cloud security
  - Key future trends we must monitor to keep the cloud secure
  - How to apply this knowledge to your own organization and the advocacy you should undertake to secure the cloud ecosystem

Tech consumerization…

- Cloud & Internet of Things, changing the world

"Frankly, I didn't expect to be so precise."

Gordon Moore
Intel co-founder and author of Moore's law

"In 20 years, every physical item will have a chip implanted in it"

Marc Andreessen
Author of first popular Web browser

CSA Maxims

- As **IT** moves into the **Cloud**, so must **Security**
- As **IT** loses control of the endpoint, **Cloud** is the only **Security** option
- As the **Internet of Things** scales upwards, **Cloud** computing will be its data repository, application engine, provisioning system, **Security** platform and organizing concept
- The security industry is being “Cloudified”

CSA Top Threats to Cloud for 2016

1. Data Breaches
2. Compromised Credentials and IAM
3. Insecure APIs
4. System and App Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. APTs
8. Data Loss
9. Due Diligence
10. Nefarious Use and Abuse
11. Denial of Service
12. Shared Technology Issues

Top Threats™ To Cloud Computing

https://cloudsecurityalliance.org/group/top-threats/

What has changed in our view of the threats?

- Insufficient Identity, Credential and Access Management
  - **Primary proximate cause** for cloud-based data breaches
  - Identity systems must scale, must be granular, *must be accurate at any point in time – on demand*
  - Multifactor authentication must be pervasive
  - Centralized storage mechanism containing data secrets (e.g. passwords, private keys, confidential customer contact database) is an extremely high-value target for attackers

Top Threats™ To Cloud Computing

What has changed in our view of the threats?

- Insecure Interfaces and APIs
  - “DevOps” agile speed of development leading to carelessness
  - Migrating legacy apps to cloud is exposing poor practices, e.g. hardcoded credentials
  - Provenance of API services is unknown
  - “Exposed” nature of APIs make them a popular attack target

Top Threats™ To Cloud Computing

What keeps the Enterprise up at night?

Cloud in the Enterprise 2016

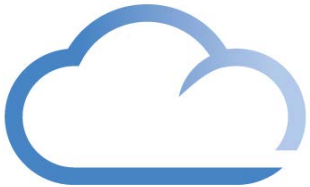
- Awareness: Capturing data on current cloud usage within organization
- Opportunistic: Identifying strong cloud adoption opportunities (Cloud First!)
- Strategic: Building cloud adoption program– security program, architecture, frameworks & business alignment
  - IaaS driving purpose-built cloud apps & the “cloudified” infosec program
  - Tackling new trends catalyzed by cloud
  - Understanding service-driven IT
  - Virtualizing the DC
  - IRON: Internet Routed Only Networks

CSA Global Enterprise Advisory Board to the rescue!

- Announced at CSA Summit @ RSA
- Chaired by Vinay Patel, Head of Security, Citi Infrastructure, Citigroup
- Public facing, demonstrate enterprise support of CSA publicly
- Issue public “Calls to action” for industry
- Advise CSA on strategy
- Issue annual “State of Cloud Security” report
  - https://cloudsecurityalliance.org/download/state-of-cloud-security-2016/
- Charter members so far: BP, Citigroup, Johnson & Johnson, Caterpillar, Hertz, Lucasfilm, ADP, AIG, Coca Cola, United Healthcare

Are Cloud Providers Secure?

- Uneven: Terrific Tier 1 Cloud Provider Security coexists with Poor and Unknown Provider Security
  - Discrimination is critical
- Secure Provider + Mature Customer may not equal secure relationship
  - Poor Integration & Alignment, e.g. Bring Your Own Keys
  - Communication Gaps, e.g. sharing event info
  - Enterprises want a holistic risk-based view of IT with Cloud as a seamless extension
- Greater transparency will help enterprises close the gaps

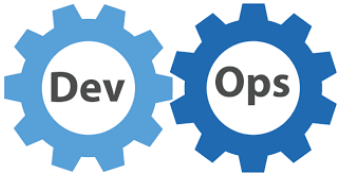


Cloud Providers Must Make Cooperation a Priority

- Threat intelligence and incident sharing
- Transparency on verifiable controls with strong integrity checks
- Standards development on common security requirements
- Support for multi-vendor enterprise: CSA enterprise users average over 1,000 unique cloud services!

Cloud is Changing the Very Nature of Information Security

- Servers are Dead, Long Live Services!
- APIs, Automation, Agility, Disposable Infrastructure
- SDN, IoT, Analytics, Cloud Access Security Brokers
- Better Ways to Handle Old Problems



National, Regional & Industry-Specific Regulations Provide Important Challenges

- Policies rapidly outdated by technology changes
- Duplicative nature of many regulations
- Conflicting regulations
- Global nature of enterprises and cloud providers vs regional regulatory authorities
- Knowledge gaps for regulators and auditors in addressing cloud computing
- Data sovereignty a difficult issue with multi-national corps
- *Engagement with Regulatory Decision Makers Key!*

Industry Skills Gap

One million unfilled information security jobs

Lagging skillsets among the employed

How do we move forward?

Fight the legacy mindset!

- 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

What have leading organizations learned?

- Due diligence is critical – ask the provider the right questions
- Understanding different types of Clouds and your Role
- Identity is very important
- Forcing legacy tools & architectures on cloud security problems doesn't work
- Heavy-handed blocking of cloud services backfires on infosec
- Key role of intermediaries
- Scale forcing greater automation

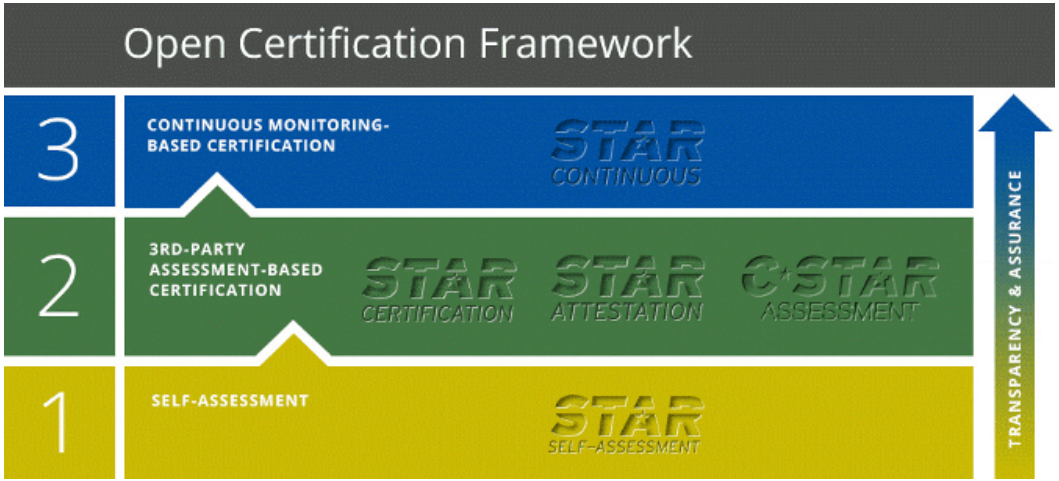
What are leading organizations doing?

- Implementing cloud security intermediaries such as CASB: Cloud Access Security Broker
- Applying security to DevOps and DevOps to security
  - "Do it yourself" scripting of orchestration tools to automate ACLs, extraction of security logs, scaling up of secure machine images
- Progressive Identity & AAA strategies
- Mandating IT security professionals upgrade their skillset
- Engaging regulators to create a reasonable path to cloud
- **Security as a Service!**

CSA STAR Provider Assurance

- Largest cloud assurance program worldwide
- Managed by CSA, delivered by leading ISO certification bodies & audit firms
- Widely accepted by industry & gov't

CSA STAR™
Security, Trust & Assurance Registry



Mad Skillz are Good Too!

- Combining vendor neutral cloud security skills with platform-specific knowledge
- Investigating next generation container and microservice tools
- Many IT security professionals enhancing (sometimes “dusting off”) coding skills to build
- Be **Hands On!**

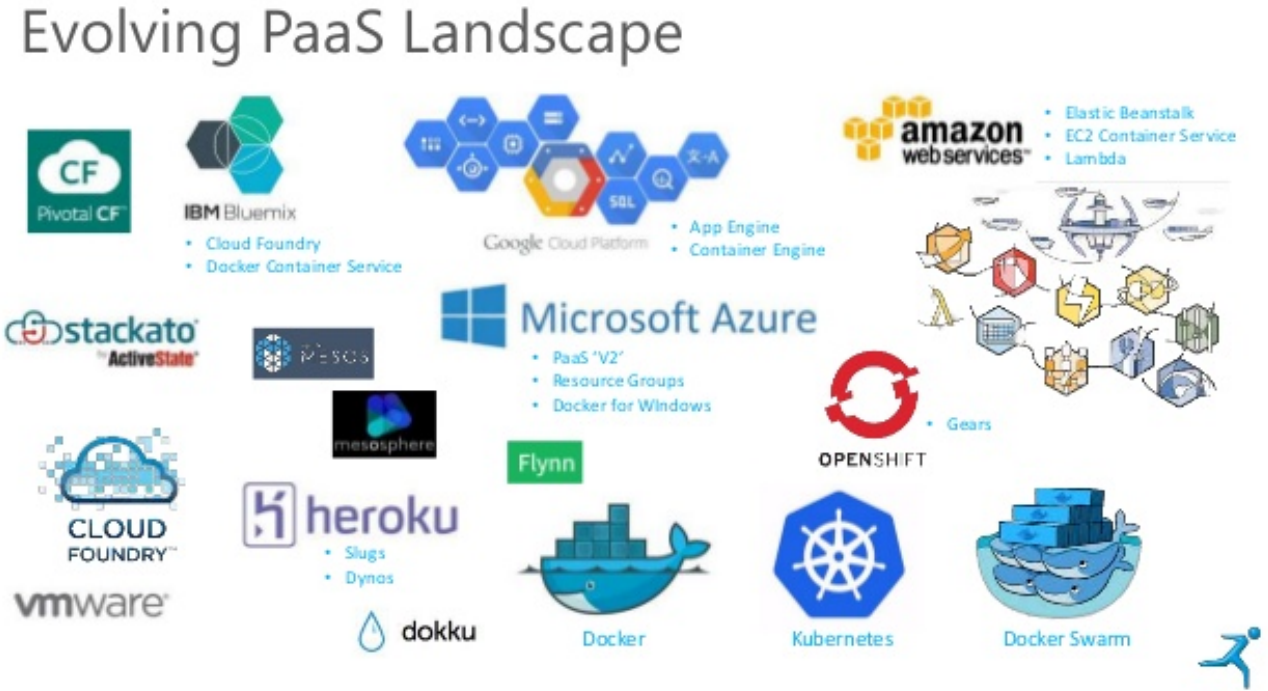
CCSK™
Certificate of
Cloud Security Knowledge

CCSP℠

cloud security alliance®

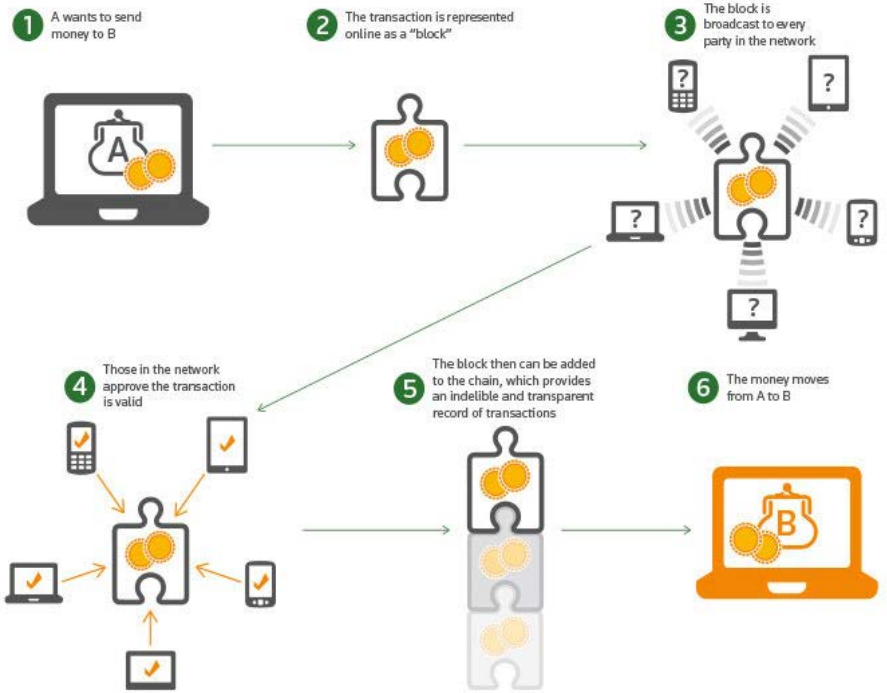
What does the future look like?

Is the Virtual Machine an enduring atomic unit of cloud?



What are the possibilities of Blockchain?

- Far beyond Bitcoin
- Distributed immutable logging has interesting applications
- Financial services looking into marrying with traditional currencies
- Applies to cloud auditing and assurance programs
- Building “web of trust” with IoT devices

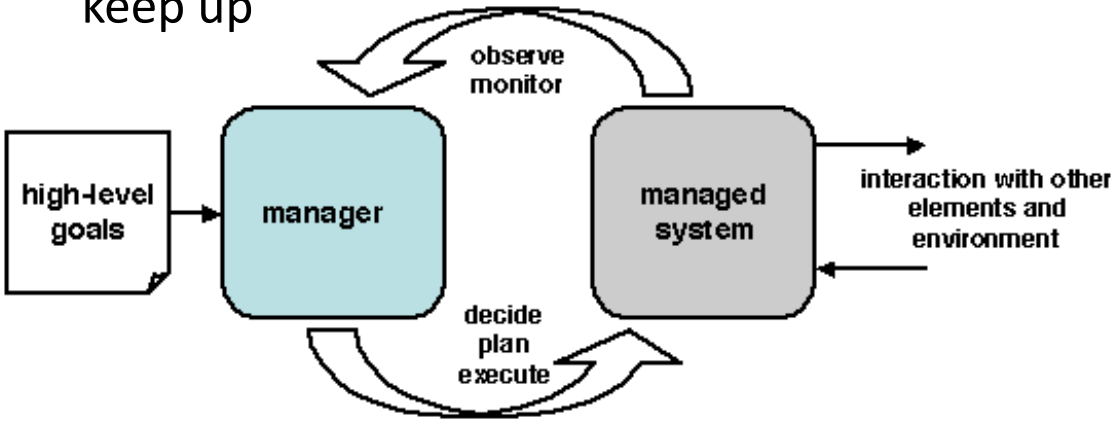


Quantum Safe Computing

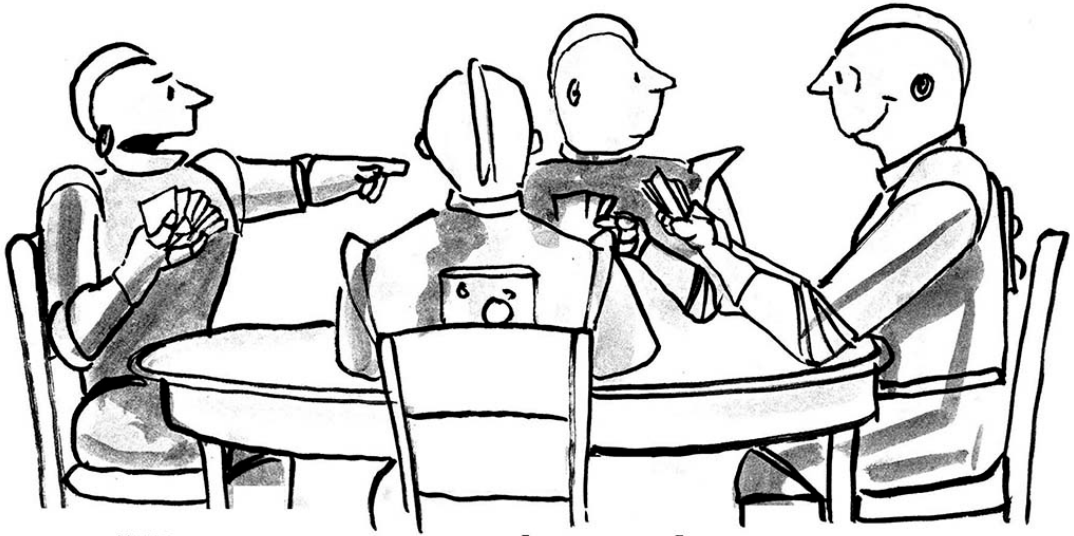
- NASA demonstrates quantum computer in December
- How long will our commercial cryptosystems be safe?
  - New cryptosystems take years to develop

Autonomic Computing

- Sensing, Adaptive, Self-Optimizing
- Monitor-Analyze-Plan-Execute architecture
- Moving humans to the periphery when they can't keep up



Artificial Intelligence



"Hey, my sensors detect that you are scanning my cards!"

Do we need a sense of urgency of the future?

- Humans cannot scale with the dual growth of Cloud + IoT
- Technology breakthroughs may threaten existing security best practices
- It takes a long time to perfect security best practices (e.g., designing a new cryptosystem)
- Developers driving innovation and dictating the future

How do you apply this to your organization?

- Realize you are not going to the cloud – you are already there
- Be demanding in your due diligence
  - Ask your providers the necessary questions – CSA STAR is an excellent model – demand transparency
  - Engage internal audit and regulators to educate them on cloud
- Visibility – if providers don't have logging & APIs, approximate it (e.g. CASB)
- Strong Identity Strategy (multi-factor, granular, realtime, microsecond integrity)
- Educate yourself, your staff on the latest (DevSecOps, Containers, Blockchain, AI, etc)
- Influence the future, it is coming fast!

RSA Conference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: CMI1-R03

THANK YOU!
State of Cloud Security 2016

Jim Reavis
CEO
Cloud Security Alliance
@cloudsa

#RSAC