Security in knowledge

NAILING CLOUDSECURITY WITH PRE-CLOUD SECURITY THINKING?

Joerg Fritsch

GARTNER

RSA CONFERENCE EUROPE 2013

Session ID: ARCH-W10

Session Classification: Intermediate

Agenda

- What is in place: Visions, Models & Commercial Offerings.
- Security Measures in Computing Clouds: a technology S-Curve.
- How to get to the sweet spot?
- Cloudsecurity: DOs and DON'Ts
- Nailing Cloudsecurity with …?

What is in place.

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

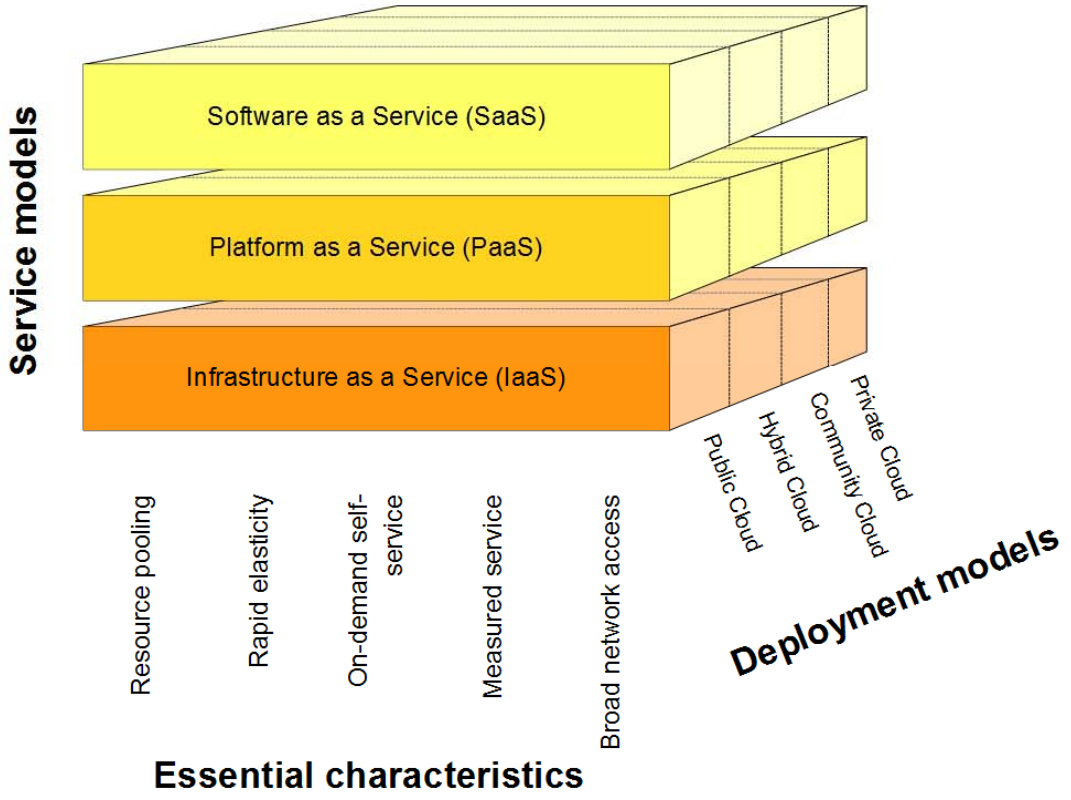
Visions

- Cloud Computing.
- Utility Computing.
- Pervasive Computing & the Internet of Things.
  - Frequently dominated by Peer-to-Peer technologies.
  - Mobile Devices.
  - Sensors.
- BIG Data.
  - “Data is the new oil”.
  - 3V Data: Volume, Velocity & Variety (Gartner, 2001).

Models & Commercial Offerings (1)

Illustration of NIST SP-800-145

Adapted from Craig-Wood 2010



Models & Commercial Offerings (2)

- IaaS: Virtual Systems.
  - Currently the dominant deployment model.
  - Virtualized copies of their legacy ancestors.
  - "All" legacy security measures are applicable. – But maybe they defy the idea (of cloud computing)?
  - VM centric security measures.
- PaaS: Application runtime (containers).
  - Under the hood: traditional software stacks maintained by the provider (such as LAMP).
  - App and Data Centric security measures applicable.
- SaaS: "Everything" else by definition & scope.
  - Avoid the fragmentation of enterprise services ("one trick solutions")

Models & Commercial Offerings (3)

- Application Services.
  - Consumed from services / application you run in an IaaS or PaaS cloud.
  - Security frequently depends on API- and SSH Keys.
  - Examples:
    - DBs, Key-Value Stores
    - Message Queues
    - SMTP
    - Storage!
    - Map Reduce and Data Analytics

Security Goals: Parkerian Hexad

- CIA triad (Owens and Tipton, 1986) not sufficient to cover computing clouds and BIG Data.
- Parkerian Hexad (Parker, 2002):
  - Confidentiality
  - Availability
  - Integrity
  - Possession
  - Utility
  - Authenticity

Threats: What is new? (1)

- Misuse or disclosure of API keys.
  - Account and/or Service Hijacking.
  - Eavesdropping, manipulating data, …
  - All service security depending on the security of these APIs.
- No perimeter.
  - Attacker can have guest VMs on the same physical platform.
    - Classic reconnaissance attacks used to "map" public clouds and achieve co-residence.
    - Covert channels.
    - Lack of entropy.
  - Consequence of multi tenancy.
- Lack of transparency.

Threats: What is new? (2)

- (Reputation) Fate sharing.
  - You may not be the source of unacceptable use but suffer from the consequences.
- Some good news: there is no NoSQL injection.

Threats: What is a déjà vu? (1)

- Cloud deployments and cloud based services inherit the security issues from the applicable domain.
  - SOA security.
  - Key management.
  - … and they also inherit the security measures.
    - For example Web Application Firewalls (WAF).
- Insider Threats.
  - Applicable to all flavors of outsourcing.
- (D)DOS
- Hypervisor exploits.

Threats: What is a déjà vu? (2)

- Availability.
  - AWS December 24 2012 outage.
    - Developer ran maintenance process against running system.
    - The developer had just returned from a DevOps conference?
  - Windows AZURE leapfrog day bug (Feb 29 2012).
  - Notion to take & compensate loss evolves!
- Scalability issues.
  - Security measures offered in IaaS clouds (such as Firewalls, iptables, ACLs) do no scale to the same extend as "the cloud".
    - Acceleration features for firewall capabilities not present on VMs.
  - In PaaS and SaaS you assume that the underlying software stack will be scalable ("elastic") as required.

Security Measures in Computing Clouds.

Security in knowledge

#RSAC

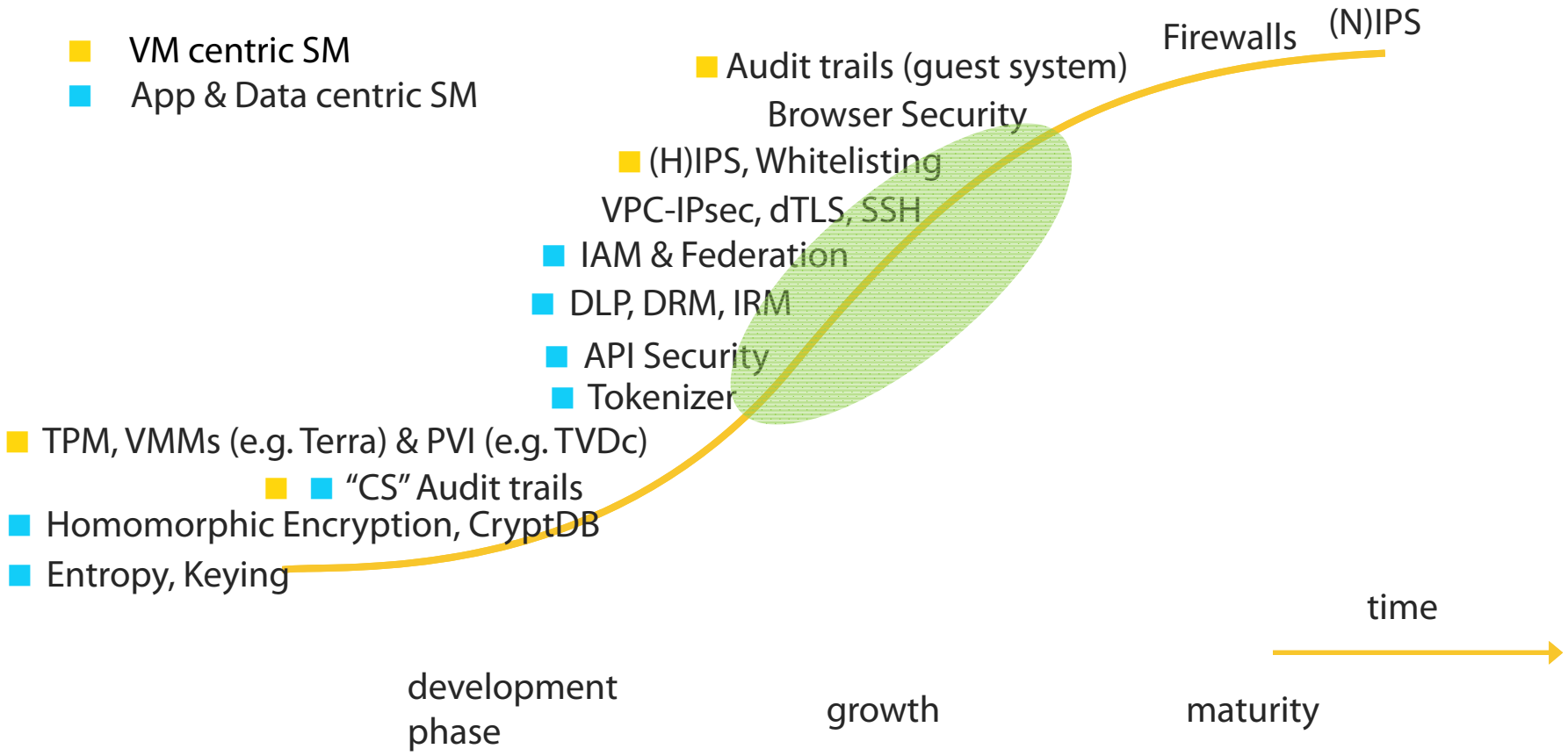
RSA CONFERENCE EUROPE 2013

The notion of security in …

- Internet, eMail, WWW, TCP/IP, C, … were all developed without having security in mind.
  - IPsec is clunky, it took 15 years before dTLS VPNs became state of the art.
  - Client to site access & tunnels overtaken by port based SSL/TLS
- WLANs had a built-in security concept (almost) from the beginning.
  - WPAv2 currently prevailing, seamless integration and adoption.
- Computing Clouds?
  - Started without notion of security. Regrettably.

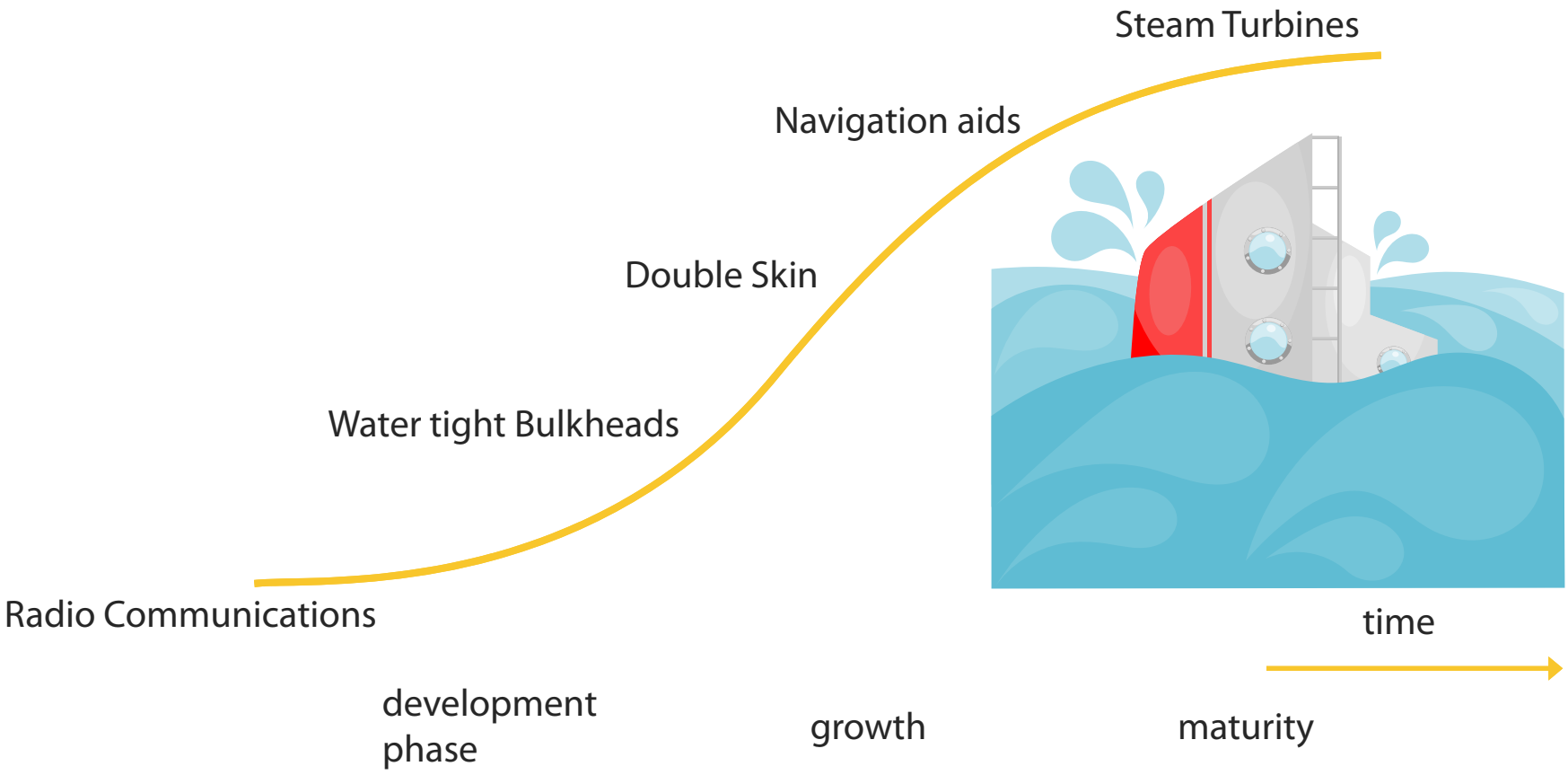
Cloud SMs on the technology S-Curve

Source: Cardiff University, School of Computer Science.

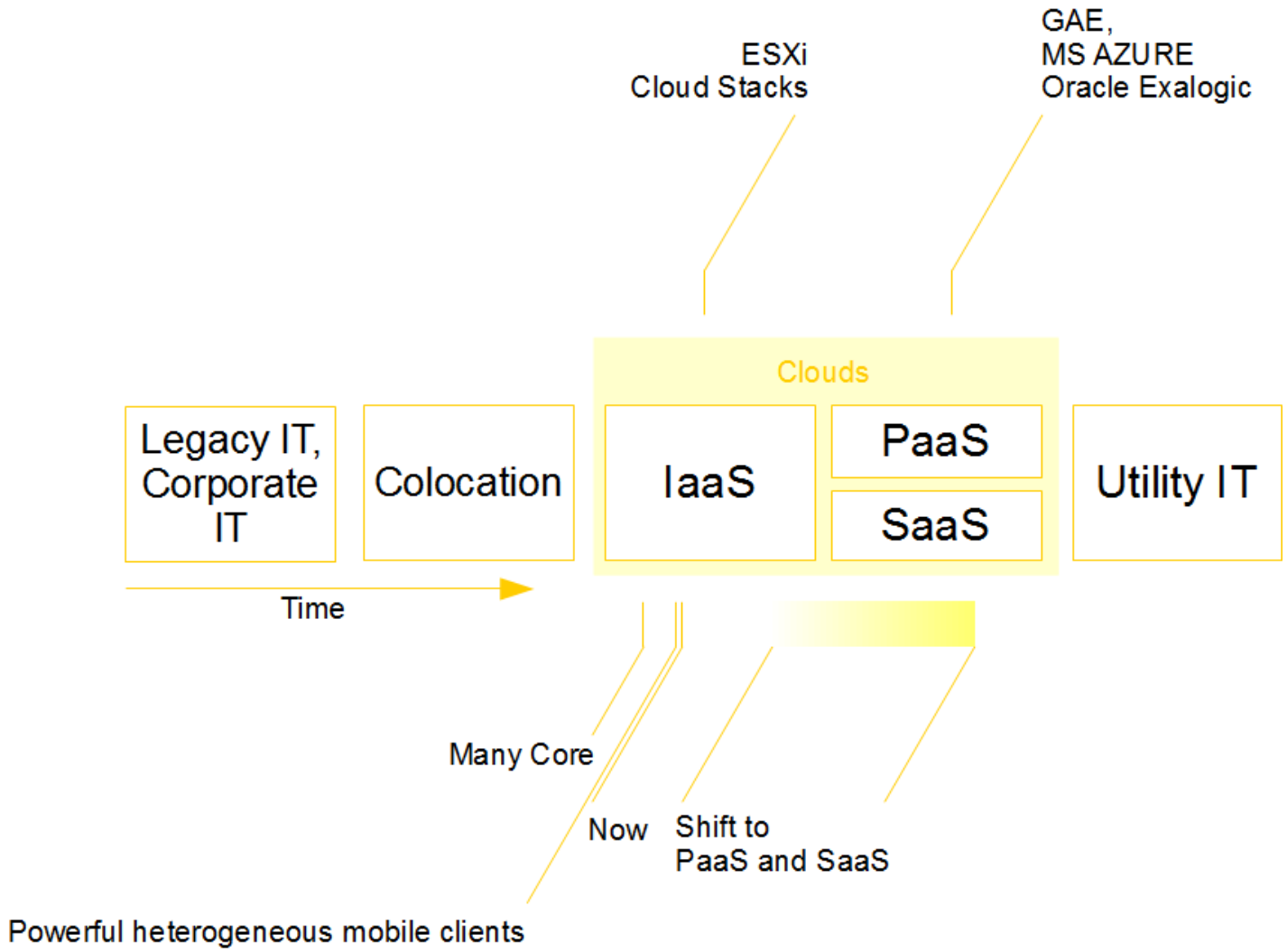


Misalignment is hard to manage

Source: Cardiff University, School of Computer Science.



IT Evolution (1)



IT Evolution (2)

- As you move to PaaS & SaaS, VM centric SMs will become less applicable.
- Network based security measures are becoming less relevant!
  - Superseded by Identity and Access Management (IAM) and federation.

How to get to the “sweet spot”?

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

Standardized Trust: Cloud SLAs

"Legacy" SLAs

- Specs & performance
- Fault Management
- Customer responsibilities

Meaningful SLAs

- Data location & segregation
- Data recovery
- Data Destruction at termination of contract
- Regulatory compliance
- Privileged user access (this is quite easy)

Change your perception of trust (1)

At home: end to end control

- Geolocation
- Data Center
- Hardware
- Code(integrity)
- OLA?

A little bit down the road: Colocation

- Geolocation
- Hardware
- Code(integrity)
- SLA

In the Cloud

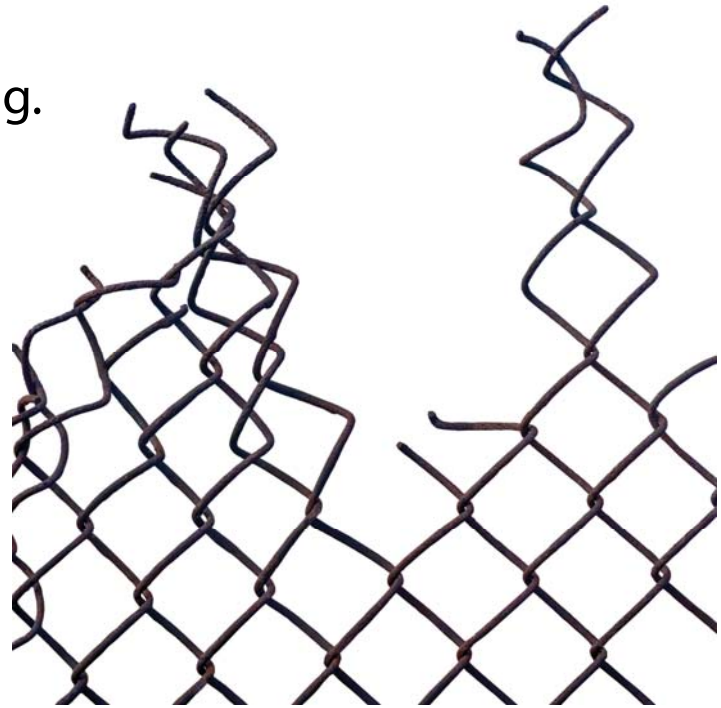
- Code(integrity)
- SLA

Change your perception of trust (2)

- Building blocks that are taken away are:
  - Replaced with new building blocks.
    - Control over the data center is replaced with an SLA.
  - Absorbed by additional security measures in the remaining building blocks.
    - Control over server hardware and software integrity can be replaced by TPM attestation/VMM and PVI.
- When "everything" is untrusted.
  - Encryption.
    - Fully Homomorphic Encryption (FHE)
    - CryptDB.
  - However, encryption alone may not even be sufficient . . . .

Let go of the perimeter

- Implementation of most new security measures may require products & talent that are not offered by your current suppliers.
- Deperimeterization now a reality.
  - Cloud Computing, Mobile Computing.
- Levels of trust can vary.
  - Everything untrusted, Semi-trusted
  - Public Cloud, Community Cloud
- "Cloud Washing" contributes to inaccurate understanding & bad decision making



Cloudsecurity: DOs and DON'Ts

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

DOs and DON'Ts

- Get the inherited application security measures right. – Realize that this is not enough.
- Don't force fit traditional notions of perimeter security to cloud computing (and mobile computing).
- Don't leave away new security measures because your current suppliers / supply chain cannot deliver it.
  - Think how to acquire new technology, skills and talent.
- Don't fall for "cloud washing". - Learn from the best in class.

DOs and DON'Ts

- Acquire deep understanding of computing clouds and the safety measures offered by "the ecosystem".
- Don't go for scattergun approaches.
- Look after your API Keys.
- Prioritize App and Data centric security measures before VM centric security measures.
- Acquire a thorough understanding of IAM & federation.
  - This is applicable to all deployment models: IaaS, PaaS and SaaS.
  - Two step authentication does not scale well and has to date only seen little exposure.

NAILING CLOUDSECURITY WITH . . . ?

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

Nailing cloudsecurity with . . .

- Pre-Cloud security thinking?
- Partially: yes.
  - Computing clouds are a disruptive innovation.
  - Programming languages and Software Stacks under the hood are not.
- Many security techniques used for Apps and Data hosted on own premises can be adapted to cloud delivery models.
- Trust issues must be compensated with new processes & technologies.

Security in knowledge

Thank you!

Joerg Fritsch

GARTNER