Toward Risk Assessment as a Service in Cloud Environments

Burton S. Kaliski Jr. and Wayne Pauley
EMC Corporation
HotCloud '10
June 22, 2010

EMC² where information lives®

Risk Assessment: Definition

- Quantitative and/or qualitative **valuation of risk** in a **specific context** against a **given threat** with a **probability of occurrence**

www.tagxedo.com

- Includes **system characterization**, **threat assessment**, **vulnerability analysis**, **impact analysis**, and **risk determination**
- Many well-established standards for assessing security; some for privacy as well

EMC² where information lives

Risk Assessment in the Cloud: Challenges

Cloud Characteristic (per NIST)	Challenge
On-Demand Self-Service	• Human interaction is replaced with **automated controls –** which now must be "trained" to pass security audits
Broad Network Access	• **Endpoints** can be any type, location, not just a pre-approved set
Resource Pooling	• **Dynamic allocation**, **virtualization** mean that resources are not known in advance • **Multi-tenancy** brings threats "in house" • **Location independence** introduces significant diversity in applicable laws

Risk Assessment in the Cloud: Challenges

Cloud Characteristic (per NIST)	Challenge
Rapid Elasticity	• **Cloud bursting** engages multiple levels of sub-providers, who must also be assessed
Measured Service	• **Metering information** has more detail about multiple tenants – a higher-value target

- **Economics** of the cloud also complicate assessments:
  - **cloud infrastructures will be constantly changing** due to market growth, M&A – risk assessments will rapidly become stale
  - **cost competition may discourage investment** in risk assessments while **increasing risk-taking**

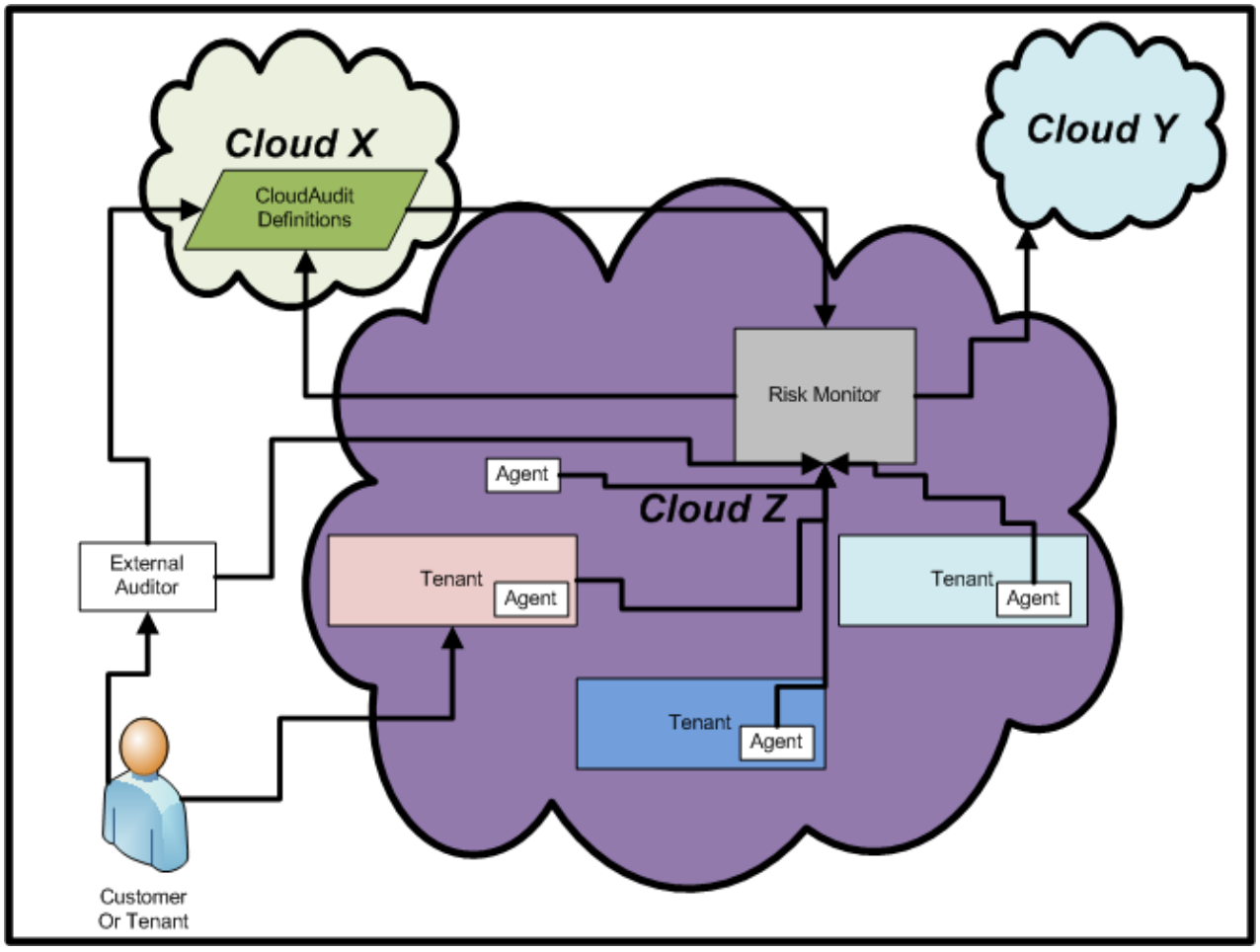
EMC² where information lives

Proposal: Risk Assessment as a *Service*

- Approach: an **automated "risk score"** (e.g. like "credit score")
  - for a given tenant or application – or for general use
  - pre-assessment and on-demand
- Modes: **provider self-assessment**, **third-party audit**, **consumer assessment** (non-privileged)
  - internal and external agents involved
- **Policy-based IT management** translates assessment of underlying dynamic resources into overall score

EMC² where information lives

Architecture



Topics for Further Research

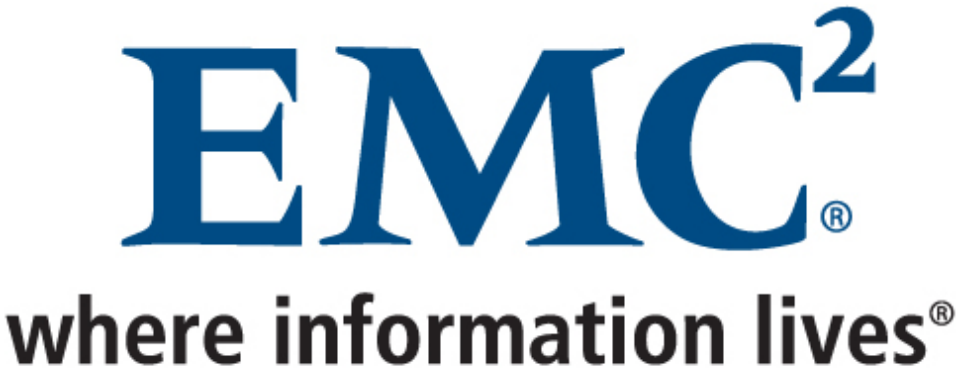
- **Automated measurement and analysis** for risk assessment
  - What sensors are needed? What language to use?
    - E.g., CloudAudit defines a dictionary based on common standards
- **Automated *adjustment*** based on the assessment
- **Trust assurances** for measurements
  - "Who guards the guards?"
- **Effectiveness of automated assessment** vs. traditional approaches

EMC² where information lives®

Contact Information

- **Burt Kaliski**
  Director, EMC Innovation Network
  Founding Scientist, RSA Laboratories
  kaliski_burt@emc.com
  community.emc.com/people/kalisb
- **Wayne Pauley**
  Director, Global Product Sales
  wayne.pauley@emc.com

EMC² where information lives


EMC²
where information lives®