RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: SEC – F02

Shadow IT – Protecting Data and Applications Outside of Your Control

Shan Zhou

VP Security Engineering
Imperva Skyfence

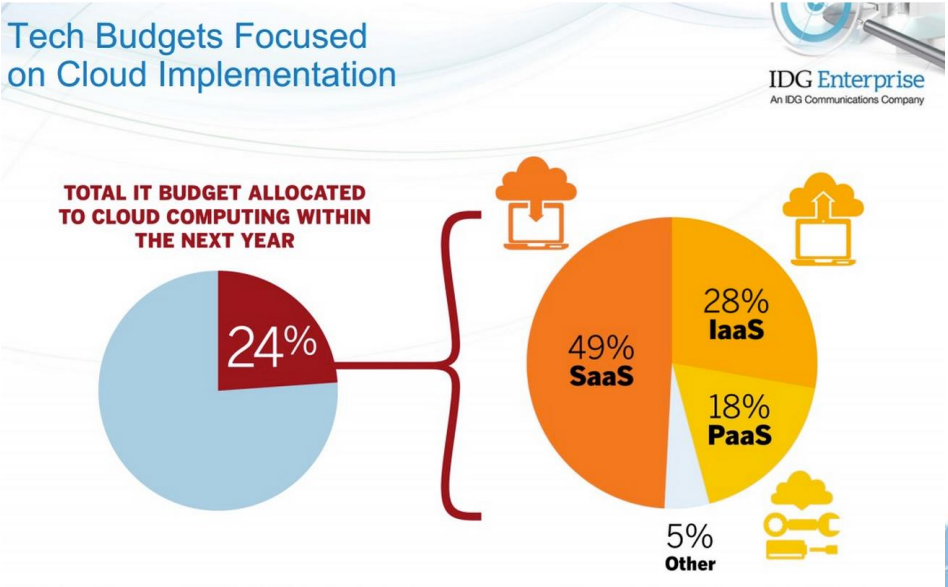
#RSAC

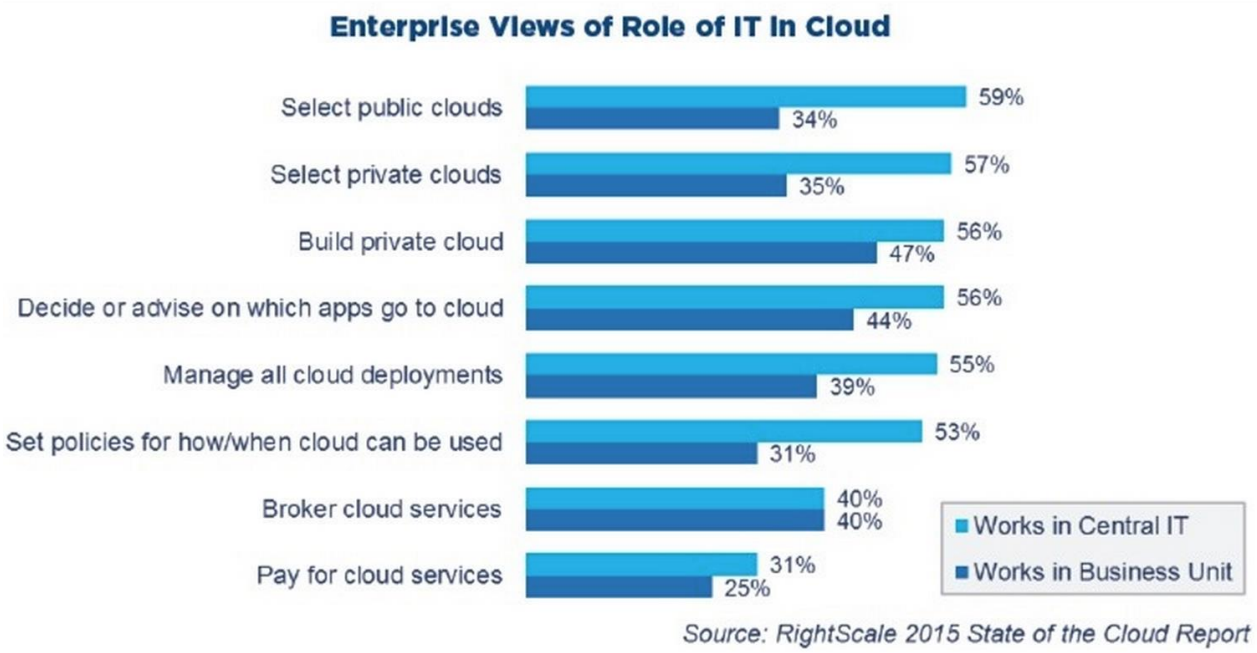
Why Cloud

Adoption Drivers

- Faster to colaboration
- Ease of trying something new
- Leveraging other experiences
- Operational efficient, focus on the business

Adoption Rate





Shadow IT Exists

Shadow IT

Adoption Drivers

- Faster to colaboration
- Ease of trying something new
- Leveraging other experiences
- Operational efficient, focus on the business

Risks

- No visibility
- Data exposure
- Lack insight into vendor policies and posture
- Compromise leads to greater compromises

Reducing Shadow IT

Adoption Drivers

- Faster to colaboration
- Ease of trying something new
- Leveraging other experiences
- Operational efficient, focus on the business

Response / Action

- Provide supported alternative
- Provide accessible environments (IaaS, PaaS) IT needs to shift to provider role
- Select products that provide hybrid offerings
- Be an enabler

RSAConference2015

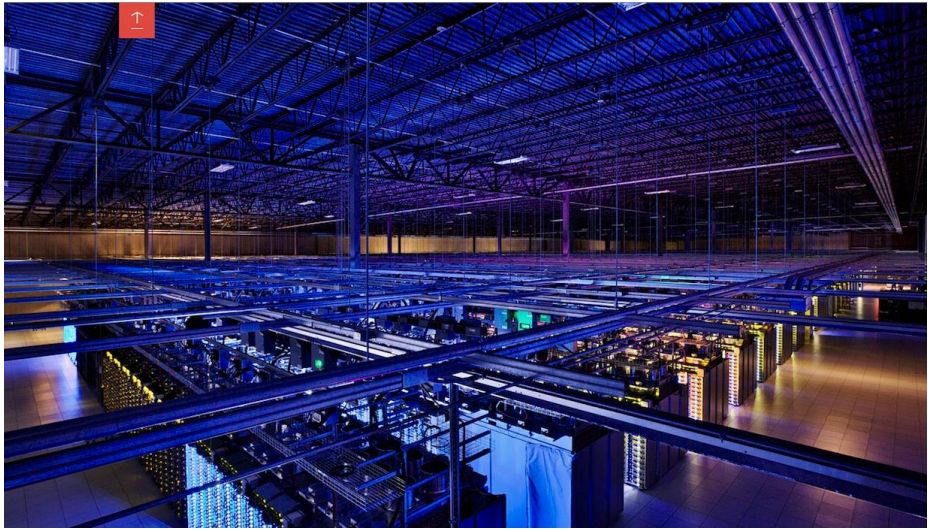
Singapore | 22-24 July | Marina Bay Sands

Cloud Security Strategy

#RSAC

What is the Cloud ?

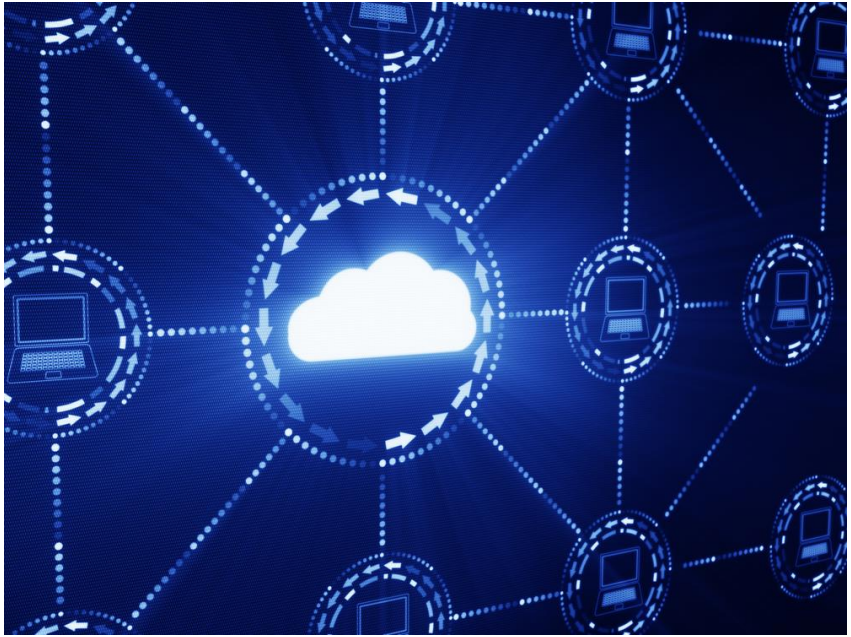
- Someone elses computer
  - Becoming aware
  - Inherent risks and implications?
  - What needs protection?



Awareness – Additional strategies to minimize Shadow IT

#RSAC

- Someone elses computer
  - Discovery includes:
    - Who
    - For what purpose
    - Why



Risks and Implications

- Someone elses computer
  - Is sensitve content involved
  - How secure is the provider / environment
  - Who has access
  - What are they doing with the data
  - Where are are they accessing it from
  - Can they take (download) data

What to protect ?

- Someone elses computer
  - Who needs protection
  - What should be protected
  - Balance / Usability

A different model

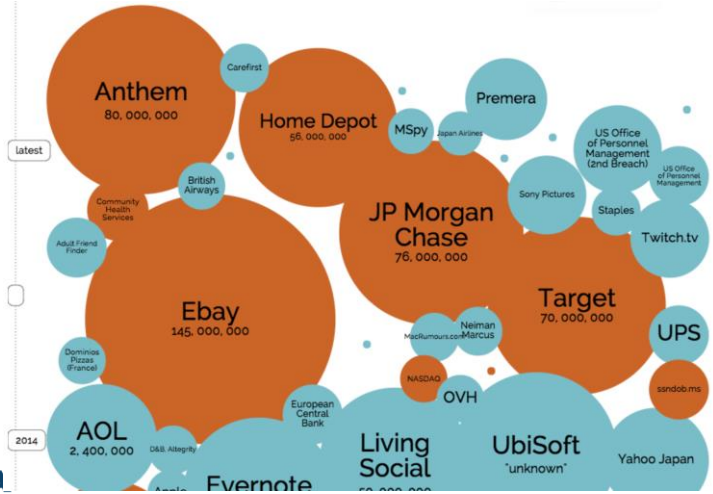
- Awareness
  - Discovery
    - Who + What = Why = Alternatives
  - Discover risk
    - How secure is vendor / provider
  - Be ready to propose alternatives

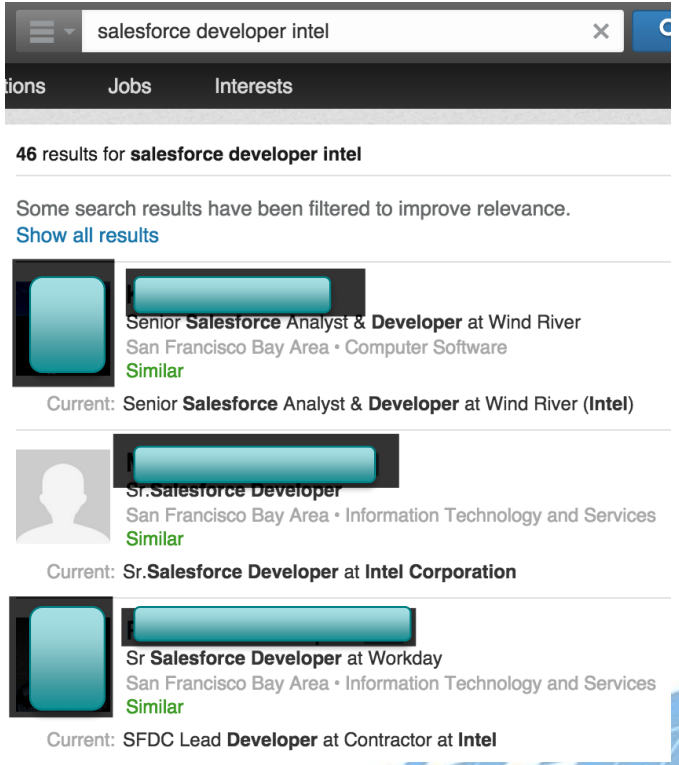
A different model

- Risk
  - Data Classification
  - Know your true risk
    - Identify configuration weaknesses
    - Privileged user monitoring
  - Control who has access
    - Least privillege model
  - Understand where the data can go

A different model

- Protection objective
  - Users
  - Devices





Use Case – Shadow IT

- Users using personal Box accounts to collaborate and share files
  - Risk
    - No control over what data is shared
    - No control where shared data is going
    - No control over who is able to share
  - Response
    - Limit who has access to data – DRM
    - Limit where data can go – file share ACL
    - Evaluate what existing alternatives exist ; Adopt Box enterprise
    - Implement controls for cloud application

Use Case – Enterprise cloud protection

- Adopted enterprise cloud email solution
  - Risks
    - No visibility into user activities
    - No method to limit what devices can connect
    - No method to verify user identity
  - Response
    - Deploy cloud security solution that can
      - Audit user activities
      - Block and control on a per device level
      - Enforce risk based identity verification

Apply

- A new model to address challenges in the cloud
  - Can’t apply existing models and methods to the cloud
  - Develop a framework for SaaS, PaaS, IaaS

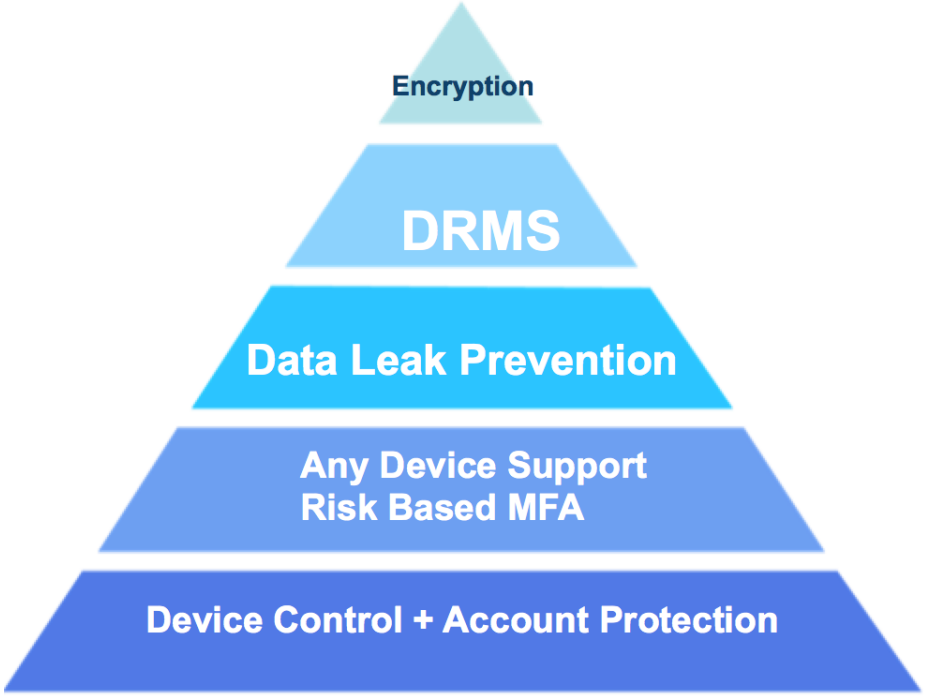
  - Discover and evaluate
    - Multiple free offerings for cloud application discovery
    - Measure vendor risk
    - Understand usage intentions
    - Identify / propose/ support alternatives

Apply

- Reduce risk
  - Passive
    - Monitor all
    - Regular assessments, know your weaknesses
  - Active
    - Protect accounts
    - Limit where data can be accessed
    - Limit where data can be stored
    - Allow but verify
    - Block, block, block

A different model

- Focus on the big problem
- Build a solid foundation
- Derive better value
- Build the stack



CASB

Cloud Access Security Brokers

- CASB named #1 in top 10 technologies for IT Security in 2014
- By 2017, those making a strategic decision to invest in cloud apps for mission-critical workloads will consider CASB essential
- The CASB market will reach $500 million by year-end 2017

CASB Use Cases

- Risk Assessment
  - Most of the market in 2014, enterprise customers, all verticals
  - Offline deployment
  - 3rd party logs, API, or web-access

Gartner

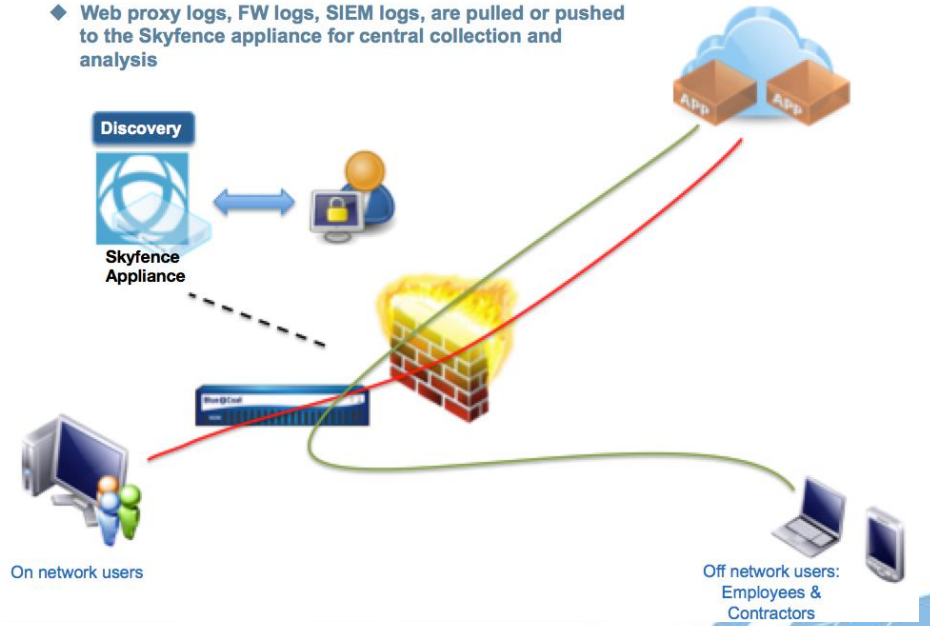
- Monitoring and Enforcement
  - Rapidly catching-up, expected 100% penetration by 2017
  - Inline deployment
  - Forward / reverse proxies, SWG integrations, endpoint agents

Developing Technologies

- Existing and developing solutions to address -
  - Shadow IT
    - Common approach - log data analysis
    - Stronger on network controls
    - Blind spot – BYOD

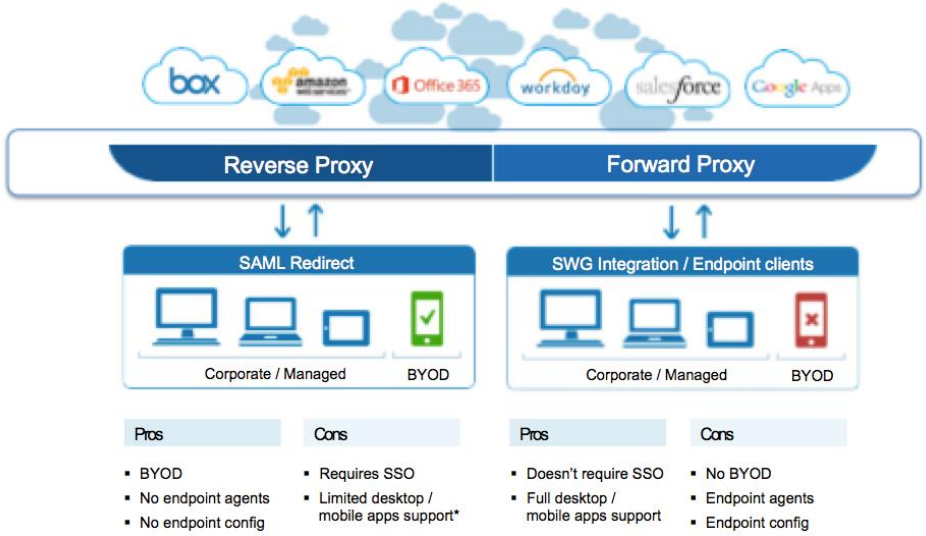
CASB Deployment Architecture

- Risk Assessment
  - Common approach - log data analysis
  - Stronger on network controls
  - Blind spot – BYOD



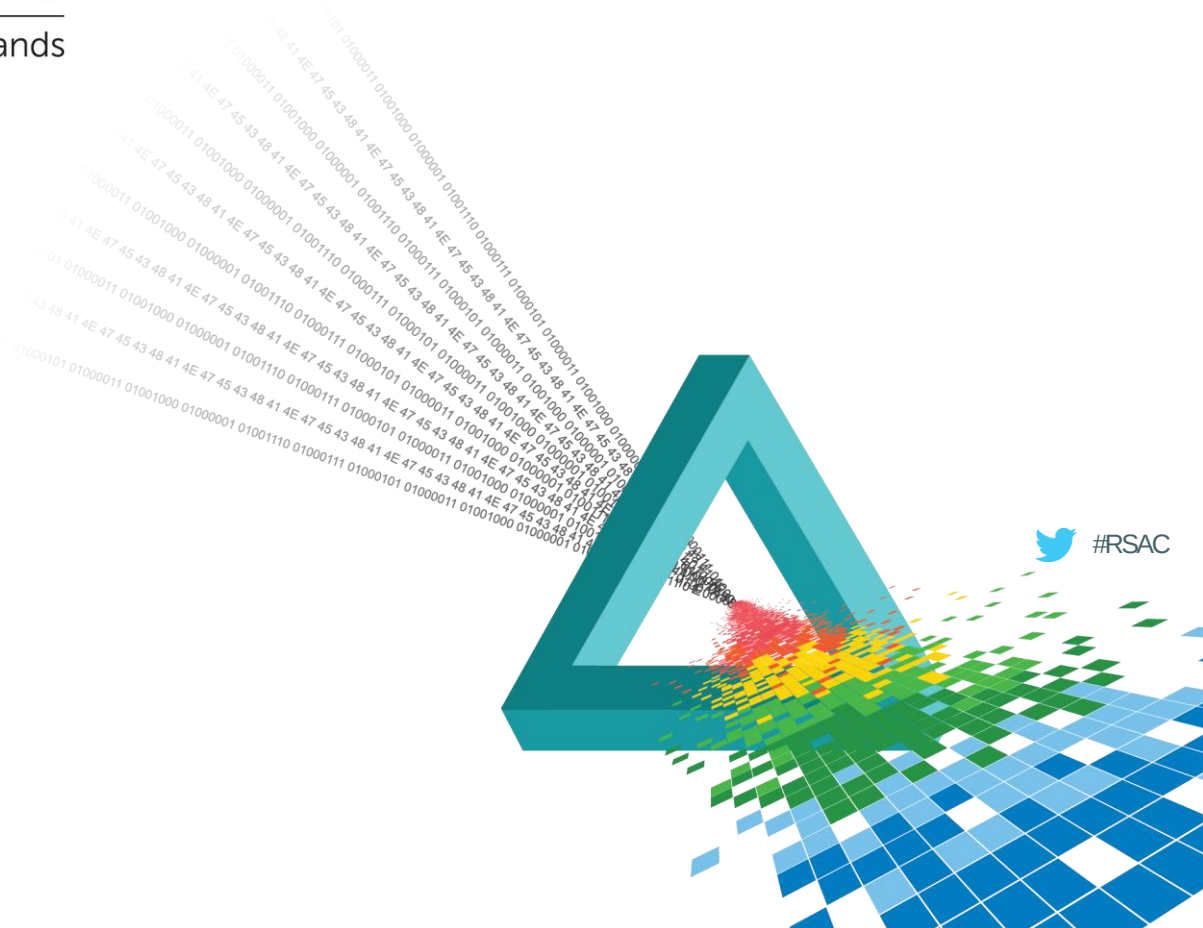
CASB Deployment Architectures

- SaaS monitoring and protection
  - API based analysis
    - SaaS vendor specific
    - Not inline – zero risk
    - No ability to interact or block
  - Inline based analysis
    - SaaS vendor specific
    - Inline risk – account for latency and availability
    - Ability to interact and block



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC