Security of Cloud Computing

Topic Overview

- Introduction
- Cloud Basics
- Securing the Cloud
- Leveraging the Cloud
- Final Recommendations

Introduction

- Cloud Computing Industry is growing
  - According to Gartner, worldwide cloud services revenue is on pace to surpass **$56.3 billion** in 2009, a **21.3% increase** from 2008 revenue of $46.4 billion, according to Gartner, Inc. The market is expected to reach **$150.1 billion in 2013**.
- Businesses are increasing Cloud adoption
  - "We expect a great deal of migration towards cloud computing within the federal government in addition to the already robust private sector growth. The growth of the cloud should not outpace our ability to protect the data that goes into it..." ~ *Former White House advisor Paul Kurtz, partner with Good Harbor Consulting, LLC*
- How can IT leaders ensure security in the cloud?

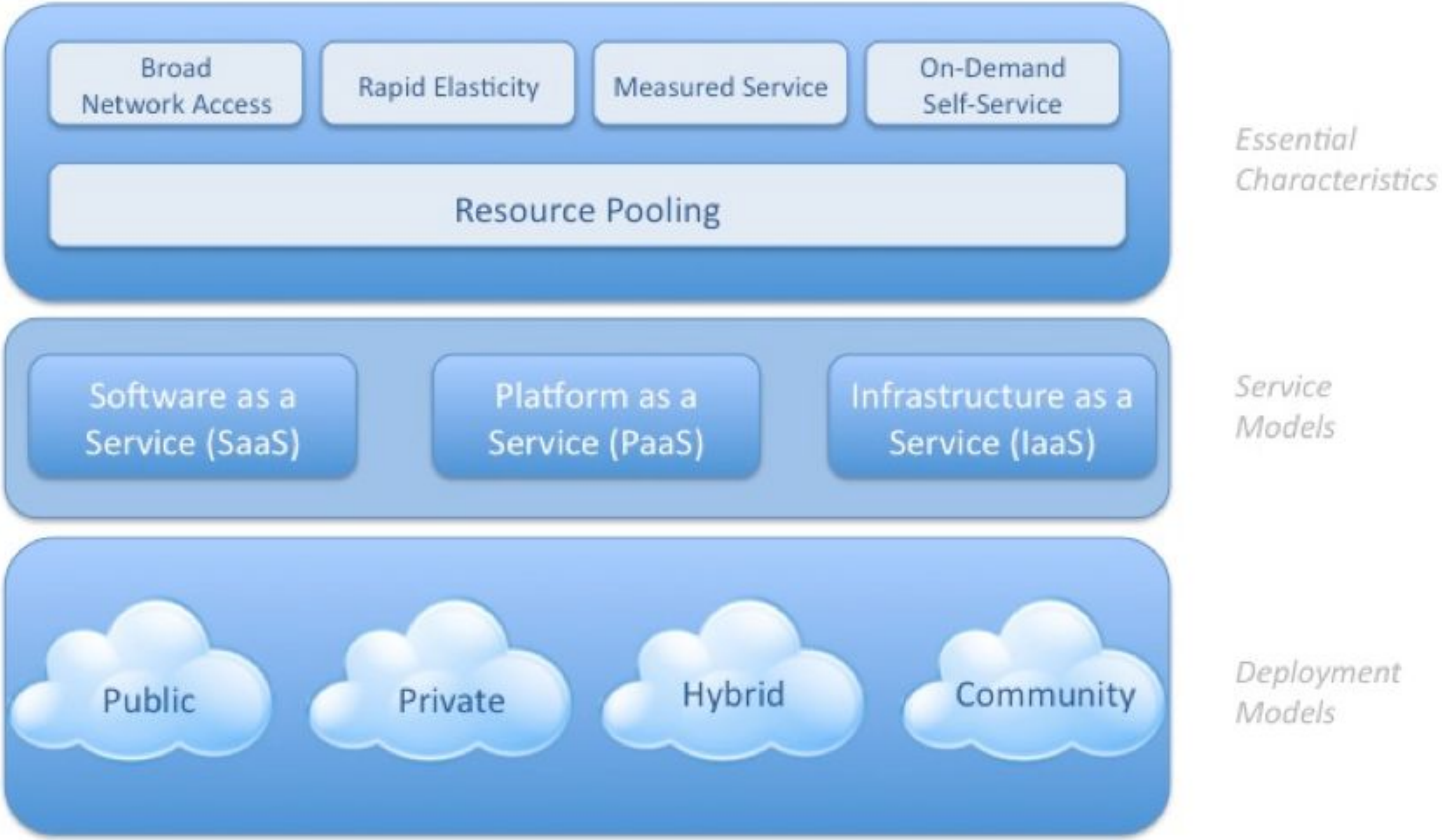
Cloud Basics

- Cloud Characteristics
- Service Models
  - SaaS
  - IaaS
  - PaaS
- Deployment Models
  - Public
  - Private
  - Community
  - Hybrid

Cloud Characteristics

Visual Model Of NIST Working Definition Of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Resource Pooling

Essential Characteristics

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Service Models

Public

Private

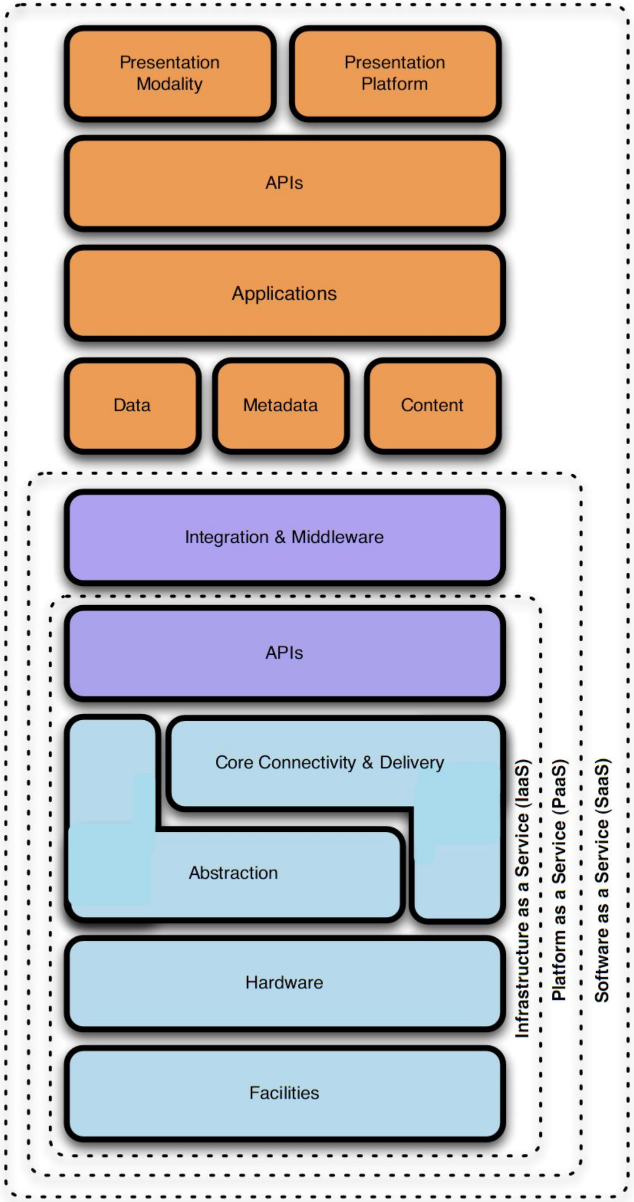
Hybrid

Community

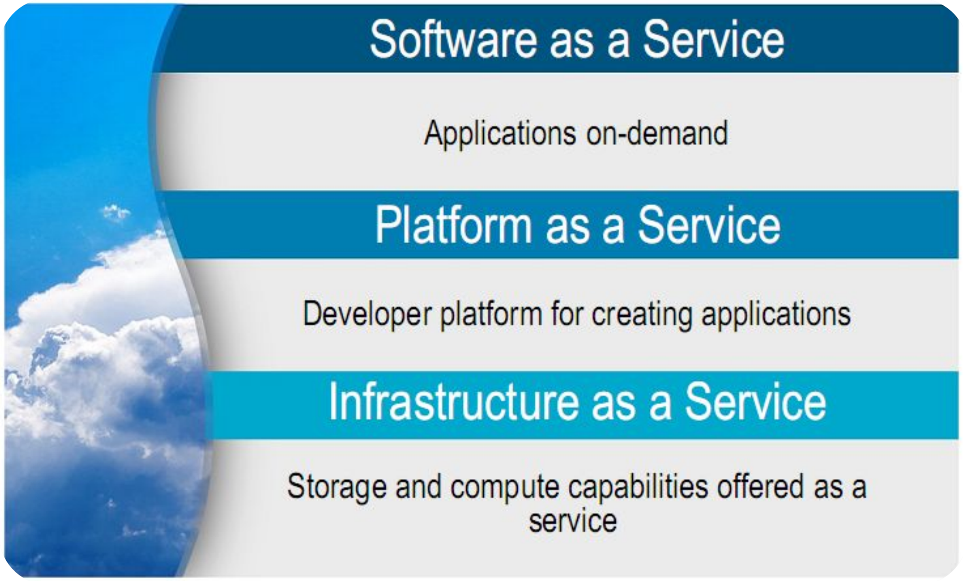
Deployment Models

Cloud Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)



Natural Evolution of the Web



Software as a Service

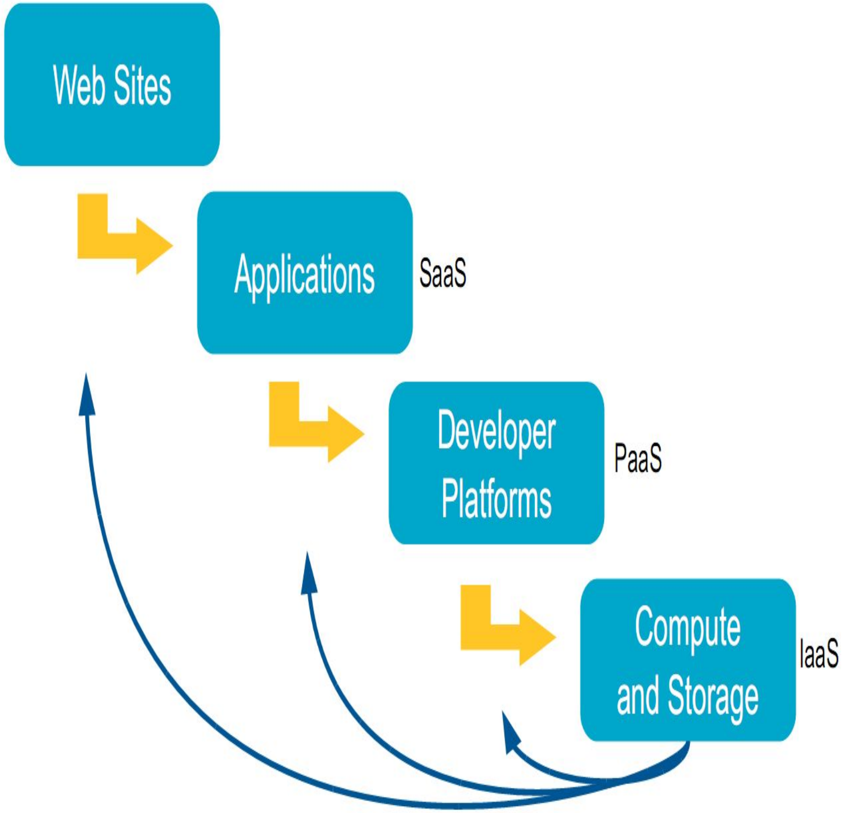
Applications on-demand

Platform as a Service

Developer platform for creating applications

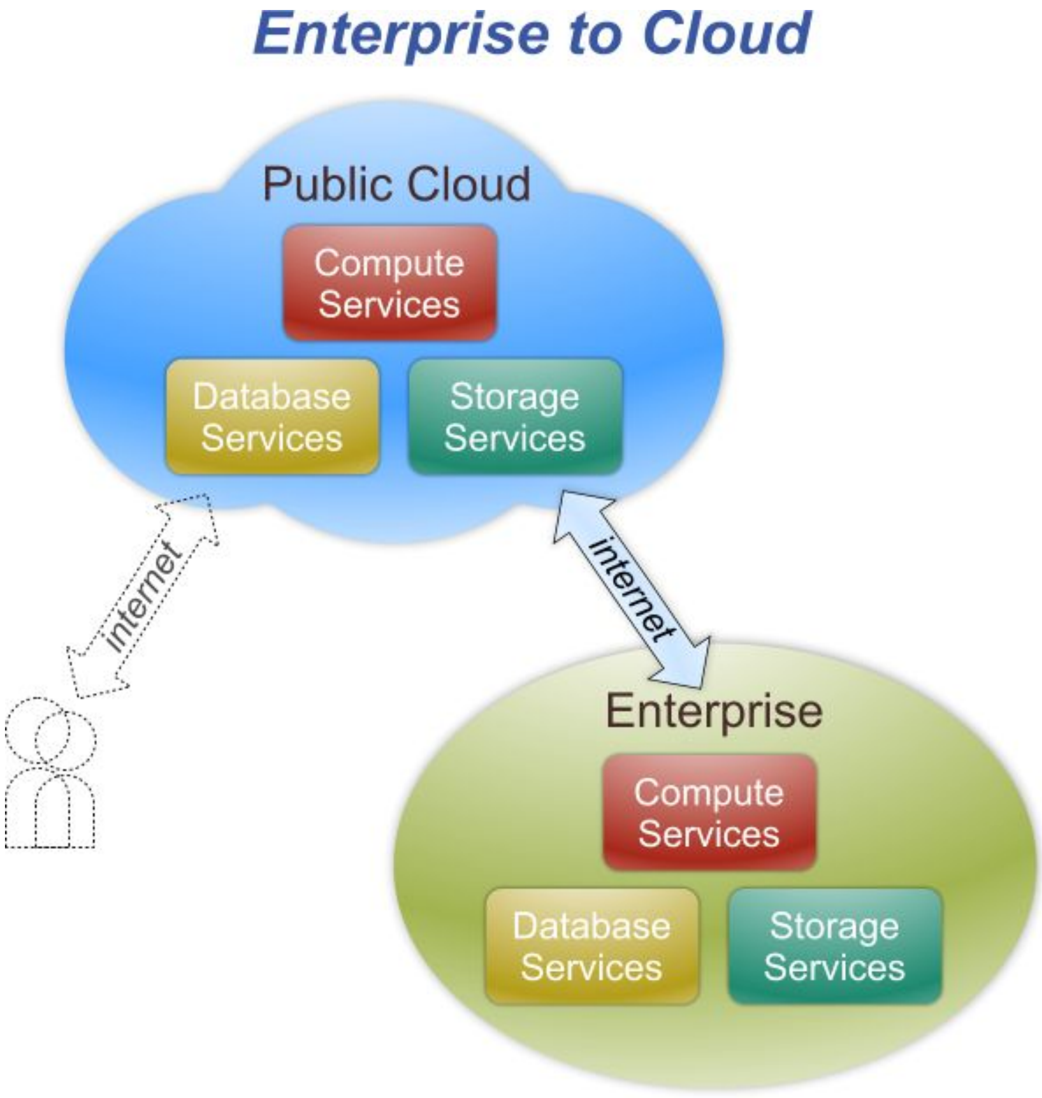
Infrastructure as a Service

Storage and compute capabilities offered as a service

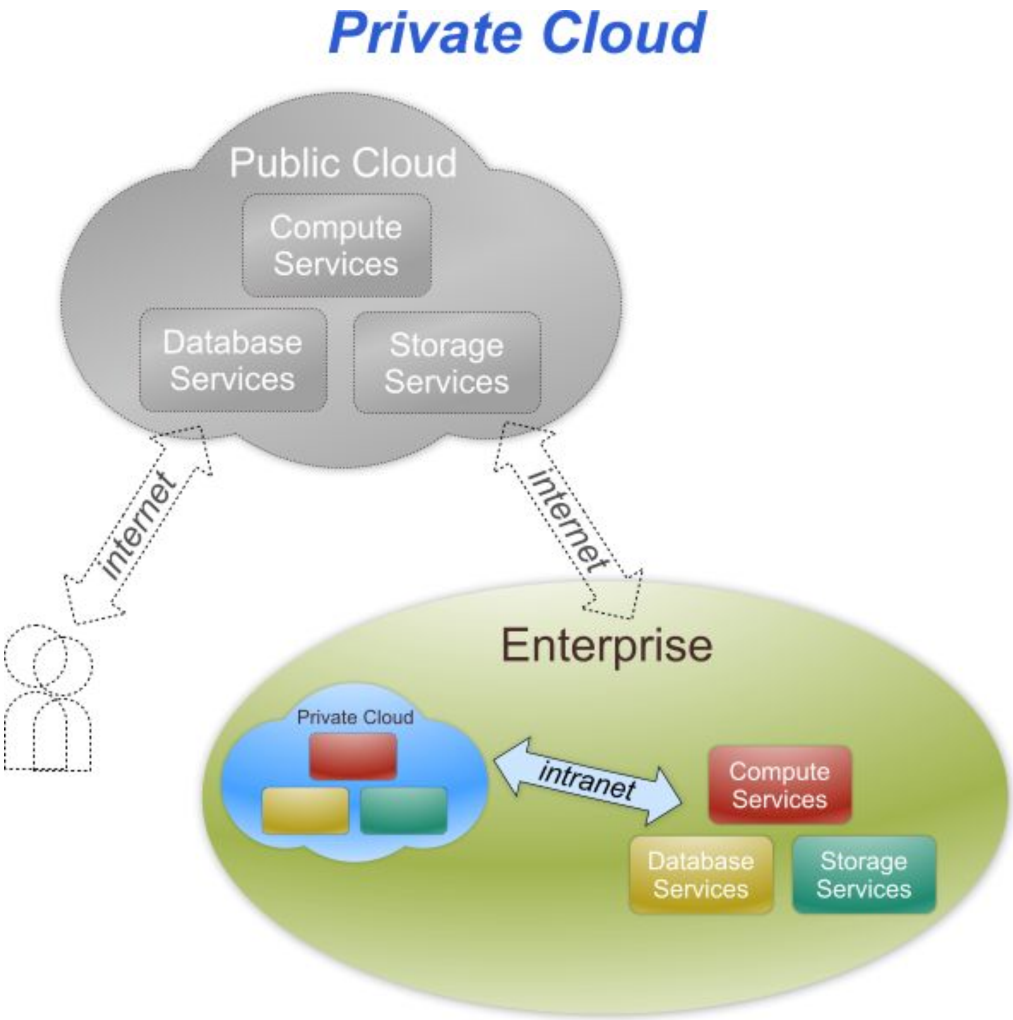


Source: Lew Tucker, Introduction to Cloud Computing for Enterprise Users

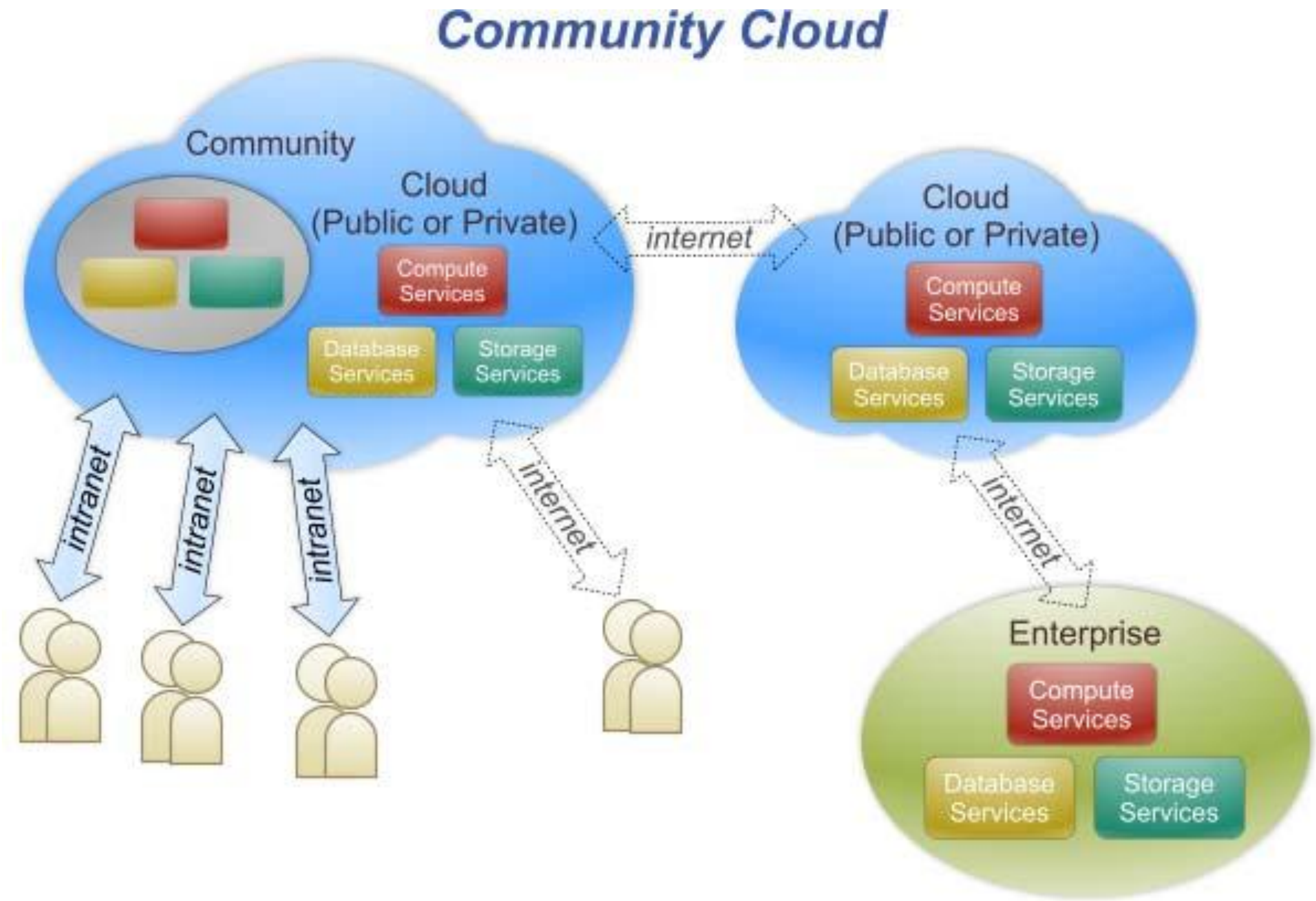
Four Deployment Models



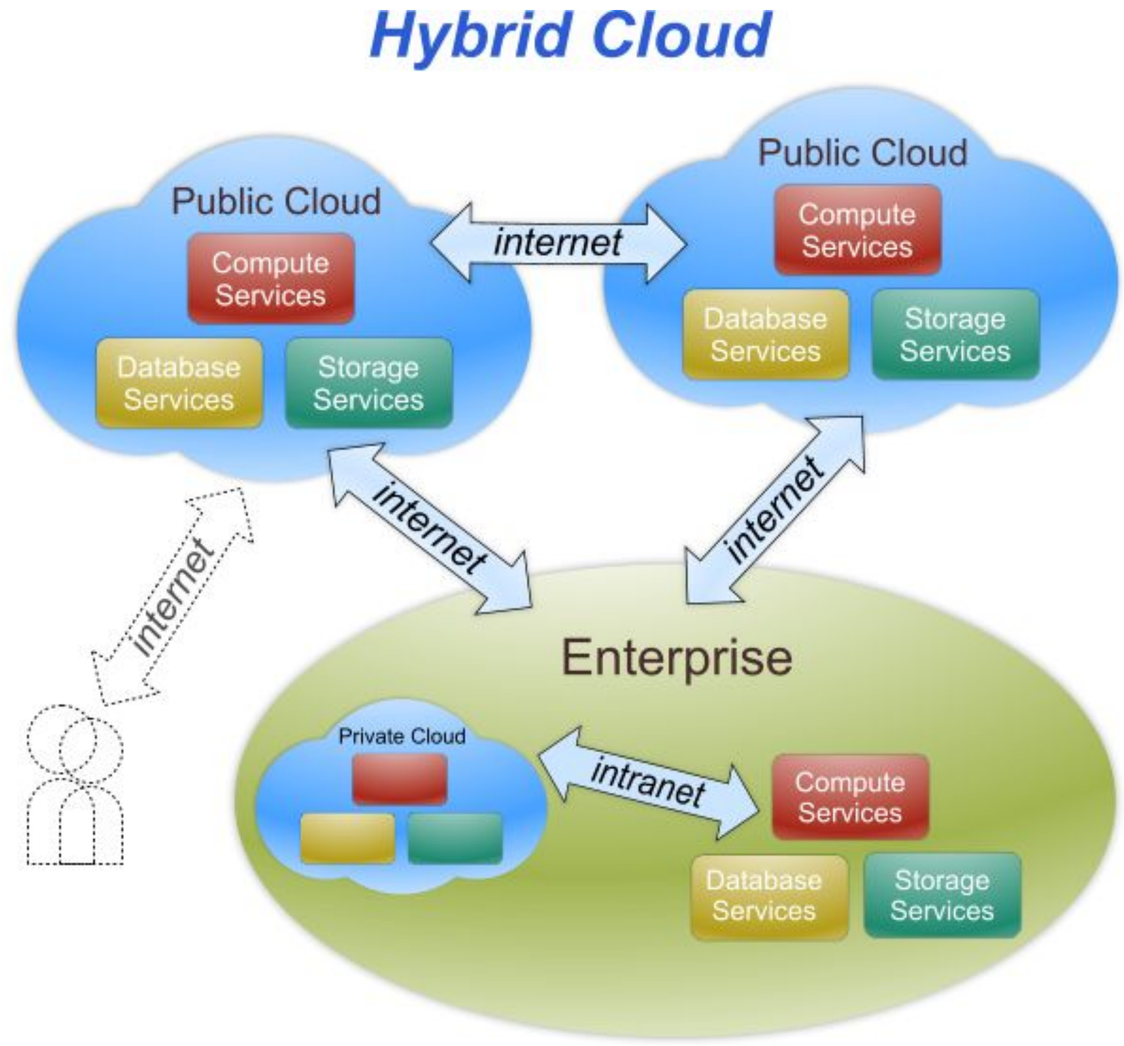
Four Deployment Models



Four Deployment Models



Four Deployment Models

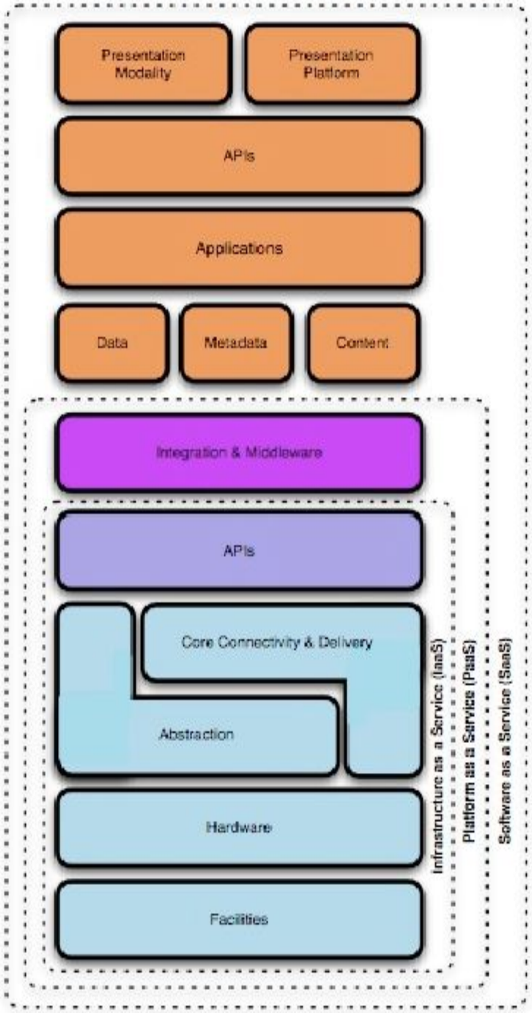


Securing the Cloud

- Security Interaction Model
- Top Security Threats
- Cloud Provider Security Practices – Google Case Study

Security Interaction Model

Cloud Model



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

Top Security Threats

- Abuse and nefarious use of cloud computing
- Insecure interfaces & API’s
- Unknown risk profile
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking

Threat Mitigation

Abuse and nefarious use of cloud computing	▪ Stricter initial registration and validation processes. ▪ Enhanced credit card fraud monitoring and coordination. ▪ Comprehensive introspection of customer network traffic. ▪ Monitoring public blacklists for one’s own network blocks.
Insecure interfaces & API’s	▪ Analyze the security model of cloud provider interfaces. ▪ Ensure strong authentication and access controls are implemented in concert with encrypted transmission. ▪ Understand the dependency chain associated with the API.
Unknown risk profile	▪ Disclosure of applicable logs and data. Partial/full disclosure of infrastructure details ▪ Monitoring and alerting on necessary information.

Threat Mitigation

Malicious insiders	▪ Enforce strict supply chain management and conduct a comprehensive supplier assessment. ▪ Specify human resource requirements as part of legal contracts. ▪ Require transparency into overall information security and management practices, as well as compliance reporting. ▪ Determine security breach notification processes.
Shared technology issues	▪ Implement security best practices for installation and configuration. ▪ Monitor environment for unauthorized changes/activity. ▪ Promote strong authentication and access control for administrative access and operations. ▪ Enforce service level agreements for patching and vulnerability remediation. ▪ Conduct vulnerability scanning and configuration audits.

Threat Mitigation

Data loss or leakage	▪ Implement strong API access control. ▪ Encrypt and protect integrity of data in transit. ▪ Analyze data protection at both design and run time. ▪ Implement strong key generation, storage and management, and destruction practices. ▪ Contractually demand providers wipe persistent media before it is released into the pool. ▪ Contractually specify provider backup and retention strategies.
Account or service hijacking	▪ Prohibit the sharing of account credentials between users and services. ▪ Leverage strong two-factor authentication techniques where possible. ▪ Employ proactive monitoring to detect unauthorized activity. ▪ Understand cloud provider security policies and SLAs.

Google Security Practices

- Organizational and Operational Security
- Data Security
- Threat Evasion
- Safe Access
- Privacy

Google Organizational and Operational Security

- Holistic approach to security
- Security team
- Develop with security in mind
- Regularly performs security audits and threat assessments
- Employees screened, trained
- Works with security community and advisors

Google Data Security

- Google Code of Conduct – “Don’t be evil.”
- Physical security
- Logical Security
- Accessibility
- Redundancy

Google Threat Evasion

- Spam and virus protection built into products
- Protects against application & network attacks

Google Safe Access

- Avoids local storage
- Access controls
- Encrypted connections
- Integrated security

Google Privacy

- Privacy policy
- Does not access confidential user data
- Does not alter data
- Maintain own IP rights
- Indemnification, liability
- End of use

Leveraging the Cloud

- Decision Making Process
- Clan Wars Case Study

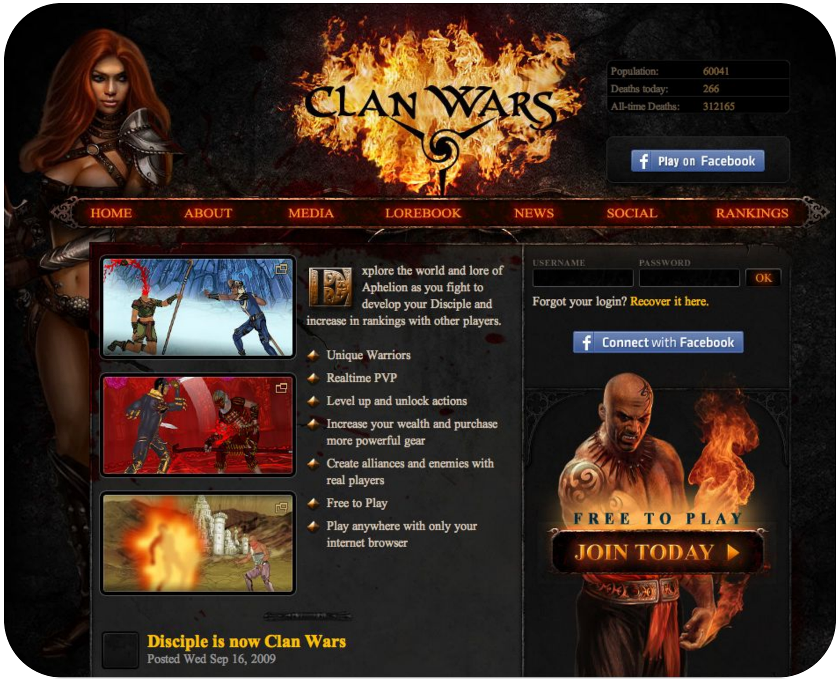
Decision Making Process

- Identify the asset for cloud deployment
- Evaluate the asset requirements for confidentiality, integrity, and availability
- Map the asset to potential cloud deployment models
- Evaluate potential cloud service models and providers
- Sketch the potential data flow
- Draw conclusions

Case Study: Clan Wars

Company Profile

- Online multiplayer game
- In Browser Flash
- Processes credit card payments



Population: 60041
Deaths today: 266
All-time Deaths: 312165

Explore the world and lore of Aphelion as you fight to develop your Disciple and increase in rankings with other players.

- Unique Warriors
- Realtime PVP
- Level up and unlock actions
- Increase your wealth and purchase more powerful gear
- Create alliances and enemies with real players
- Free to Play
- Play anywhere with only your internet browser

Forgot your login? Recover it here.

Disciple is now Clan Wars
Posted Wed Sep 16, 2009

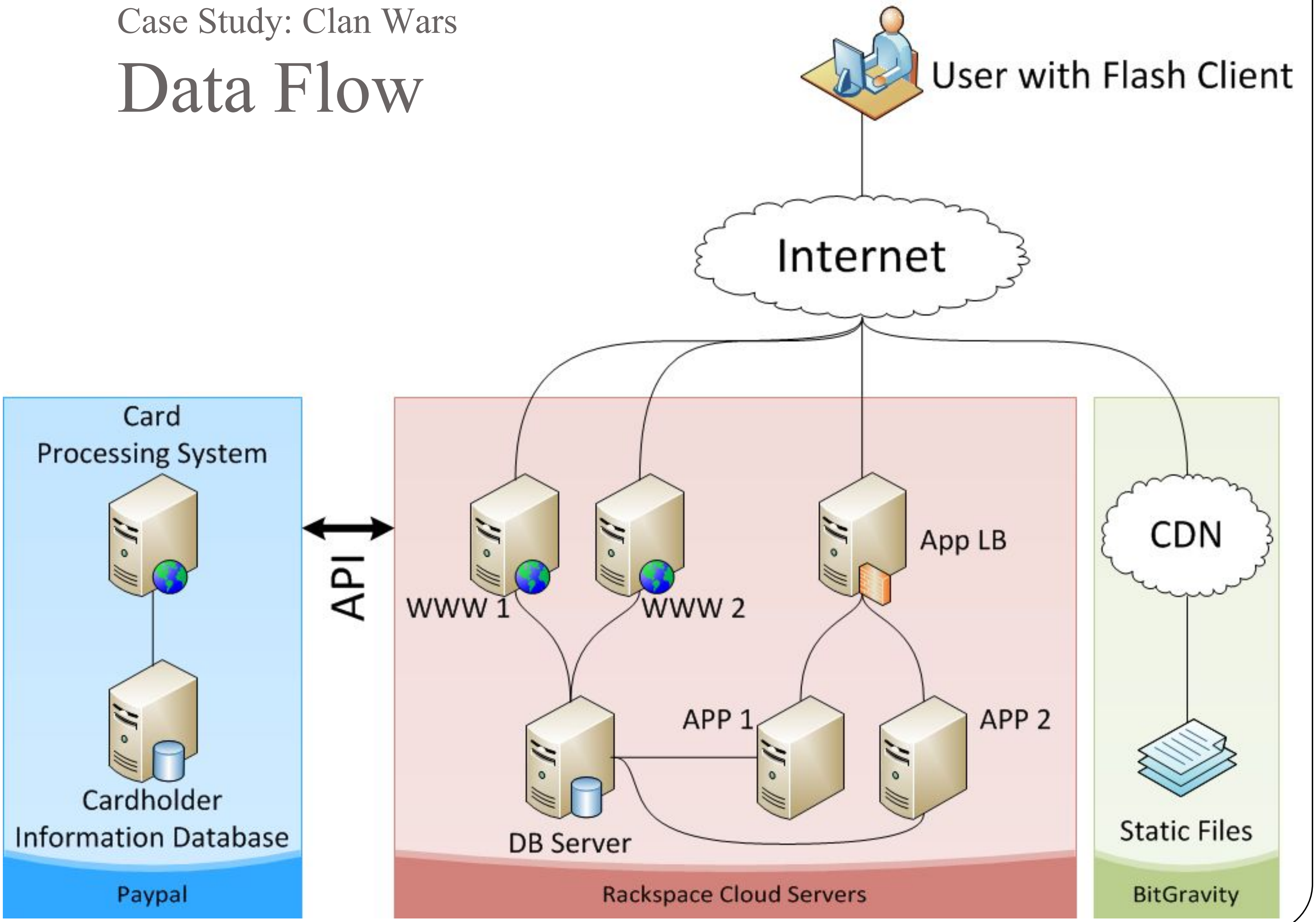
Case Study: Clan Wars

Decision Making Process

- Identified all components as candidates
- Evaluation concluded:
  - Payment = High concern on all factors
  - Game & data = Medium on all factors
- Primary components mapped:
  - Infrastructure (Servers, storage, etc)
  - Payment Processing
  - Collaboration

Case Study: Clan Wars

Data Flow



Case Study: Clan Wars

Conclusion

- Great fit
  - Risk requirements met
  - Data flow supports needs
- Added benefits
  - Low cost (saving ~$500/month)
  - Low maintenance
  - Performance

Final Recommendation

- No universal answer
- Evaluate your security needs versus the capabilities of the provider

Q & A

Supplemental Material

- The sections that follow will not be covered during the presentation but are included for reference.

Rackspace Security Practices

- Physical Security
- System Security
- Operational Infrastructure Security
- Client Application Security

Cloud Consumer Best Practices

Governance Domains

- Governance & Enterprise Risk Mgmt
- Legal and Electronic Discovery
- Compliance and Audit
- **Information Life Cycle Management**
- Portability and Interoperability

Operational Domains

- Traditional Security, Business Continuity, and Disaster Recovery
- Data Center operations
- Incident Management
- **Application security**
- Encryption & Key Mgmt
- Identity & access Mgmt
- Virtualization