Cloudy with a Chance of Pain

EXPLORE | INNOVATE | LEAD

Online BUSINESS SYSTEMS

A few quick

BACKGROUND DETAILS

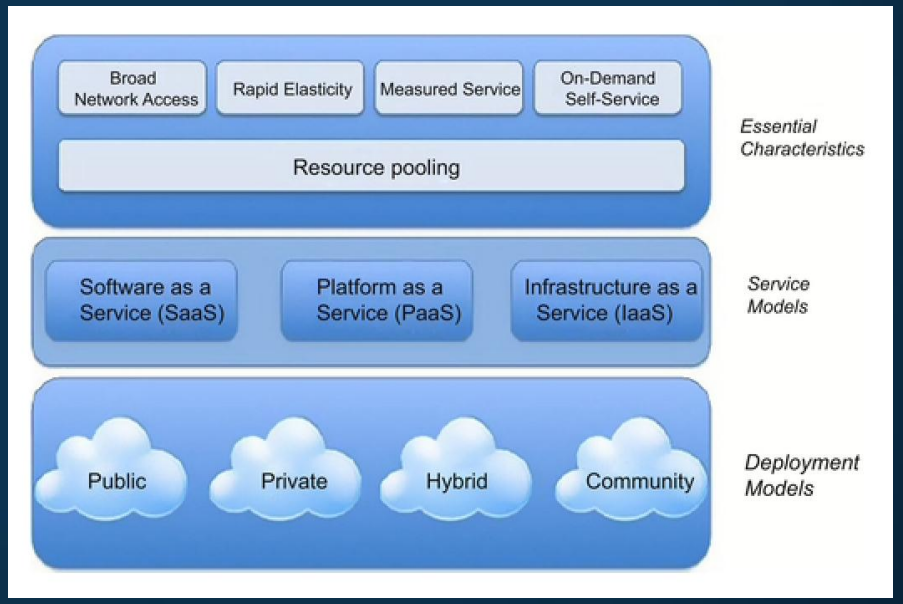
Scope of Talk

- The following discussions will be more relevant for IaaS & PaaS infrastructures than SaaS
- Public cloud vs, hybrid private
- Native tools and workflows

- There’s just no way to cover securing the cloud in 50 minutes – but we’ll do our best to cover what we think are important areas

Cultural Shift

- The cloud demands a new thought process
- From it's architecture…to usage…to security



But is it Really Different?

- Many of the same traditional principles apply
- CSA Cloud Security v3 Domains:

Architecture	Governance	Operations	
Architectural Framework	Governance and Enterprise Risk Management	Traditional Security, Business Continuity, and Disaster Recovery	Encryption and Key Management
	Legal Issues: Contracts and Electronic Discovery	Data Center Operations	Identity and Access Management
	Compliance and Audit	Incident Response, Notification, and Remediation	Virtualization
	Information Management and Data Security	Application Security	Security as a Service
	Interoperability and Probability		

Going Native?

- The cloud platforms are developing and maturing
- Features are being introduced at a rapid pace
- Pros:
  - ↳ Always available
  - ↳ Standard interface
  - ↳ Largest community of users
  - ↳ Backed by the provider
- Cons:
  - ↳ Limited to offerings provided
  - ↳ May not be able to add functionality
  - ↳ Additional cost
- For now, we'll limit ourselves to just native functionality

Determine Responsibility by Service

- Managed vs. custom
- Many services are being offered as “managed”
- Managed services typically provide a more simple management interface, but limit control for complex environments
- Generalism vs. customization
- Examples: Active Directory, NAT

Due Diligence

- Before you move to cloud…

Data Awareness	What's in/moving to the cloud?	Data Inventory & Classification
System Awareness	What systems make up the cloud?	System Inventory
Network Awareness	How does the cloud interact?	Data Flow Diagram
User/Role Awareness	Who works in the cloud?	User/Role Inventory
Risk Awareness	What are your risks to the cloud and the data?	Risk Assessment

CLOUD SECURITY BASICS

Q: What is the Best Security Framework?

- Considerations:
  - ↳ Threats
  - ↳ Vulnerabilities
  - ↳ Technical Controls
  - ↳ Governance
  - ↳ Resources
  - ↳ Cost
  - ↳ Compliance / industry requirements
  - ↳ Geo-location

A: What is the Best Security Framework?

- The one that works best for you! </groan>

- Plenty of work has been done to document security frameworks, don't work too hard!

Traditional	Cloud Adapted	Threat Based
• ISO 27001 • NIST 800-53 • NIST 800-144 • PCI DSS	• CSA Guide v3 • CSA CCM • ENISA Documents	• SANS Top 20 • Industry Breach Reports + Controls

Public Endpoints

- All traffic to public clouds inherently cross the Internet
- This is where cloud is the most vulnerable to outsiders
- Thankfully, CSPs know this is the case
- But you can give them a hand
- Limit the public footprint

Administrative Remote Access

- Admins/privileged users from external physical and network locations will need access
- Many of these users will not want/need access to the web management portal
- Provide secure access to cloud resources
- Use a jumpbox-type of solution and harden
  - ↳ SSH bastion host
  - ↳ Privileged workstation

Multi-Factor Authentication

- Available on all major public clouds
- Easiest way to reduce the likelihood of account takeovers
- Minimizes the potential impact of credential loss

Segmentation

- Use ‘VLAN-type’ controls to isolate environments
- Create multiple tiers (Internal/Ext/DMZ/etc.)

- Also segmentation on internal networks
  - ↳ This can go beyond just Dev/Test/Prod

- Don’t forget to use ACLs as well
  - ↳ ACLs limit potential vulnerabilities even further

IAM / User Management

- Initial user management can be done through the management console
- Create new users and quit using root/admin!
- Limit users who have access to platform/console
- Create strong password policies
- Use non-interactive logins for application accounts

IAM / User Management

- Bump up the control!
- Use an Identity and Access Management Tool
- Active Directory or LDAP can provide additional controls and federate with your current environment
- This can help leverage investment already made in IAM
- Especially important if you are creating a hybrid cloud with a current environment

Compute Security

- Typically select processing speed, memory, and OS
- But it's likely not hardened or available (OS updates)
- Create systems consistently with approved builds
- Some additional security controls may be available
  - ↳ Anti-malware
  - ↳ Logging APIs
  - ↳ FIM
  - ↳ HIDS
- General Rule of Thumb: Customer is responsible for OS level security

Compute Security

- Take advantage of the cloud's scalability and replace servers with new patched ones instead of updating
- Concept of Immutability
  - ↳ Once servers are pushed, no changes are allowed
  - ↳ Ensure gold standard is used
  - ↳ Allow for alerting of any changes on running compute as sign of compromise or tampering
- Containers?
  - ↳ Docker
  - ↳ AWS Service
  - ↳ Azure service (preview as of 12/2)

Storage Security

- Likely to be on of the most sensitive locations
- Generally closer to PaaS and maintained by CSP
- Create separate security group
- Encrypt the most valuable data
- Use provided Encryption Key Management

You Are Backing Up, Right?

- Availability is still a core security fundamental
- Short Term
  - ↳ High availability, easy recovery
  - ↳ Snapshots of servers
  - ↳ Backup of data to another geography
- Longer Term
  - ↳ Static, low cost storage
  - ↳ Glacier /Recovery Services

CLOUD GOVERNANCE & COMPLIANCE

You’re Not Paranoid

- Someone is likely checking up on you
  - ↳ Auditors, Assessors, Santa
- This is the function of Governance and Compliance
  - ↳ To ensure defined processes are being followed

- Good News!
- Cloud makes this easier than ever
- It just takes a little legwork

Creating Streamlined Processes

- Use existing frameworks or standards
- Security Pre-Approvals
  - ↳ Allows a limited set of configurations that are fast-forwarded through the approval process
  - ↳ Encourages usage of secure configurations
  - ↳ This is how you say yes to the business
- Automate everything
  - ↳ …and document
  - ↳ Less human intervention means more consistency and should lessen the audit requirements

Monitoring

- Monitor everything
  - ↳ Logging is available for almost any action taken
  - ↳ Send that information to a centralized system
- Develop escalation path for alerts
  - ↳ Not everything is important
  - ↳ But you can use your threat assessment to identify what should be prioritized
  - ↳ And then alert
  - ↳ This aligns with the goals of Threat Intelligence

Vulnerability Management

- Adopt continuous HOST-BASED vulnerability management
  - ↳ Scan network on any change
  - ↳ Scan compute on instantiation
  - ↳ Use Host IDS

Cloud High Priority Security Checklist

- ❑ Minimize Public Endpoints
- ❑ Secure Remote Protocols
- ❑ Enable MFA
- ❑ Segment Environments
- ❑ Quit Using Root
- ❑ Create Users and Limit Access
- ❑ Use Application Accounts
- ❑ Build Once, Deploy Many
- ❑ Harden Compute Images
- ❑ Replace, Don’t Patch
- ❑ Encrypt Sensitive Data
- ❑ Use Key Management Solution
- ❑ Create HA/Backups
- ❑ Security Pre-Approvals
- ❑ Monitor Everything
- ❑ Create Alerts
- ❑ Continuous Vulnerability Management
- ❑ Document your Security

James K. Adamson, CISSP, CCSP, CRISC, QSA
Senior Consultant, Online Business Systems

jadamson@obsglobal.com
@jameskadamson