Cloudy with a Chance of Pain

Innovation, just ahead.
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 its architecture...to usage...to security
But is it Really Different?

- Many of the same traditional principles apply

- **CSA Cloud Security v3 Domains:**

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Governance</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Framework</td>
<td>Governance and Enterprise Risk Management</td>
<td>Traditional Security, Business Continuity, and Disaster Recovery</td>
</tr>
<tr>
<td></td>
<td>Legal Issues: Contracts and Electronic Discovery</td>
<td>Data Center Operations</td>
</tr>
<tr>
<td></td>
<td>Compliance and Audit</td>
<td>Incident Response, Notification, and Remediation</td>
</tr>
<tr>
<td></td>
<td>Information Management and Data Security</td>
<td>Application Security</td>
</tr>
<tr>
<td></td>
<td>Interoperability and Probability</td>
<td>Security as a Service</td>
</tr>
</tbody>
</table>
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...

<table>
<thead>
<tr>
<th>Awareness Type</th>
<th>Question</th>
<th>Related Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Awareness</td>
<td>What’s in/moving to the cloud?</td>
<td>Data Inventory &amp; Classification</td>
</tr>
<tr>
<td>System Awareness</td>
<td>What systems make up the cloud?</td>
<td>System Inventory</td>
</tr>
<tr>
<td>Network Awareness</td>
<td>How does the cloud interact?</td>
<td>Data Flow Diagram</td>
</tr>
<tr>
<td>User/Role Awareness</td>
<td>Who works in the cloud?</td>
<td>User/Role Inventory</td>
</tr>
<tr>
<td>Risk Awareness</td>
<td>What are your risks to the cloud and the data?</td>
<td>Risk Assessment</td>
</tr>
</tbody>
</table>
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!

<table>
<thead>
<tr>
<th>Traditional</th>
<th>Cloud Adapted</th>
<th>Threat Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td>CSA Guide v3</td>
<td>SANS Top 20</td>
</tr>
<tr>
<td>NIST 800-53</td>
<td>CSA CCM</td>
<td>Industry Breach Reports + Controls</td>
</tr>
<tr>
<td>NIST 800-144</td>
<td>ENISA Documents</td>
<td></td>
</tr>
<tr>
<td>PCI DSS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 one 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