Moving to Hybrid Cloud?
It’s Time to Re-Think Security to Prevent Data Breach

Wade Tongen – Regional VP of System Engineering
Agenda – Moving to Hybrid Cloud?

1. Hybrid Cloud and Trends
2. Security threats in Hybrid Clouds
3. IAM & PAM Best Practices
Hybrid Cloud Adoption Trends

Basic
- Backups/DR
- Test/Dev
- Existing Apps

Intermediate
- New Apps
- Re-Architect or Replace Apps

Advanced
- Use Lower Level Services
- Invest in New Methodologies
- DevOps Automation
Hybrid Cloud is an Extension of Your Data Center
Hybrid Cloud Requires Privileged Access Security

“58% of all organizations surveyed are embracing cloud, with an expected growth in cloud spending of 44% over the next two years.”

IDC CloudView 2016 Survey

“Through 2020, 95% of IaaS security failures will be the customer’s fault, and more than half of those will be attributed to inadequate management of identities, access and privileges.”


93% of Organizations store sensitive data in the cloud.

A commissioned study conducted by Forrester Consulting on behalf of Centrify

“Businesses are still responsible for confidentiality, integrity, and availability of their data in the cloud.”

Shared Responsibility Model
AWS Shared Responsibility Model

Customers are responsible for their security configuration **IN** the Cloud

AWS looks after the security **OF** the cloud
Security Challenges for AWS Service Management

- **AWS Account hijacking threat**
  - Hacker puts Hosting Service Code Spaces out of business
  - “Account Jumping, Post Infection Persistency & Lateral Movement in AWS"

- **Several reported attacks target AWS Accounts**
  - Credential leak via source repositories such as Github
  - Phishing and Man in the Browser attacks
  - Compromised AMI leaks Metadata server info and credentials
  - Malicious or poisoned 3rd party AMIs (not vetted by AWS Marketplace)
  - Account leftovers in black market accounts with unused AWS credit
Secure Access for AWS Service Management

- Lock down the “root” or billing account
  - Vault the password for the AWS root account, and enforce MFA for break-glass access

- Establish Federated login for temporary access
  - Eliminate IAM Users and long-lived access keys

- Enforce IAM Role-based temporary privileges
  - Leverage AWS Role to grant the least privilege
Security Challenges for AWS EC2 Instances

• Managing access and privileges
  • How to control login to Linux and Windows EC2 Instances? With MFA?
  • How to manage access to the root or local admin account?
  • How to manage privileges of users with login access?
  • How to audit all access and privileged operations within these Instances?

• Default accounts
  • Linux default accounts - Linux instances will have an ec2-user, ubuntu or centos account depending on OS distribution and can sudo any command
  • Windows local admin account – has a randomized password You can retrieve the password with your root account’s access key
IAM Best Practices for Hybrid Cloud

Common Security Model
Leverage and extend on-premises access policies to deploy infrastructure and apps quickly and securely in AWS

Eliminate Shared EC2 Key Pairs
Minimize attack points by leveraging Active Directory, LDAP and cloud directories versus creating local accounts and managing EC2 key pairs for authentication

Ensure Accountability
Leverage existing user accounts or federate access to services and resources in AWS. Create fine-grained permissions to resources, and apply them to users through groups or roles

Least Privilege Access
Grant users just the access they need in the AWS console, on EC2 instances and to apps. Implement cross platform privilege management for AWS console, Windows and Linux

Audit Everything
Log and monitor both authorized and unauthorized activity in EC2 instances. Associate all activity to an individual, and report on both privileged activity and access

MFA Everywhere
Consistently implement MFA for AWS service management, on login and privilege elevation for EC2 instances, and when accessing enterprise apps
Cyber Attacks Target Privileged Accounts

- Current tools make it too easy to compromise privileged accounts:
  - Kali Linux enables anyone to attack – pre-loaded with all the right attack tools
  - Mimikatz extracts credentials from memory
  - Pass-The-Hash enables lateral movement using stolen NTLM hashes
  - oclHashCat can brute-force NTLM hashes at 250,360,000,000 tries per second

Targeted Attack Lifecycle
(Mandiant, A FireEye Company, M-Trends 2016)

- Initial Compromise: Gain Initial Access into Target
- Establish Foothold: Strengthen Position within Target
- Escalate Privileges: Steal Valid User Credentials
- Internal Recon: Identify Target Data
- Move Laterally: Package and Steal Target Data
- Complete Mission: Maintain Presence
REDUCE RISK WITH BEST PRACTICES FOR ACCESS

FORRESTER FINDS IMPLEMENTING IDENTITY BEST PRACTICES RESULTS IN

- 50% fewer breaches
- $5 MIL in cost savings
- 40% less on technology costs

GUIDE TO ACCESS

DANGER
- Too Many Passwords
- Too Much Privilege

GOOD
- Establish Identity Assurance

BETTER
- Limit Lateral Movement
- Require Access Approvals
- Automate Provisioning
- Minimize VPN Access

GREAT
- Enforce Least Privilege
- Just-in-Time Privilege
- Just Enough Privilege
- Don’t Break Glass

OPTIMAL
- Audit Everything
- Analyze Risk
- Monitor Sessions
- Integrate with SIEM

LOWEST HANGING FRUIT
- Consolidate Identities
- MFA Everywhere
- Risk-based Access
- SSO Everywhere

REDUCE RISK WITH BEST PRACTICES FOR ACCESS
Identity Best Practices – Minimize the Attack Surface

- Establish Identity Assurance – preventing account misuse w/ MFA and SSO
- Limit lateral movement – restrict default permissions and leverage MFA
- Enforce least privilege – temporary privilege elevation as required
- Log and monitor all privileged access
Thank You