Cloud Security

Ian Ruffell

Introduction

- Ian Ruffell
  - SAS Technical Architect

- Who's using SAS in the cloud?
  - SSOD
  - AWS
  - Softlayer
  - Private Cloud
  - Other

Types of Service

- IaaS
  - The most basic cloud-service model is that of providers offering computing infrastructure
- PaaS
  - Cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure
- SaaS
  - Software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted
- RaaS
  - Given a business problem, the provider solves it to give you a business result

Cloud Security Principals

1. Data in transit protection
   - Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.
2. Asset protection and resilience
   - Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
3. Separation between consumers
   - Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.
4. Governance framework
   - The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

Cloud Security Principals

5. Operational security
   - The service provider should have processes and procedures in place to ensure the operational security of the service.
6. Personnel security
   - Service provider staff should be subject to personnel security screening and security education for their role.
7. Secure development
   - Services should be designed and developed to identify and mitigate threats to their security.
8. Supply chain security
   - The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.

Cloud Security Principals

9. Secure consumer management
   - Consumers should be provided with the tools required to help them securely manage their service.
10. Identity and authentication
   - Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.
11. External interface protection
   - All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.
12. Secure service administration
   - The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.

Cloud Security Principals

13. Audit information provision to consumers
    - Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.
14. Secure use of the service by the consumer
    - Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.

Shared Responsibility Model

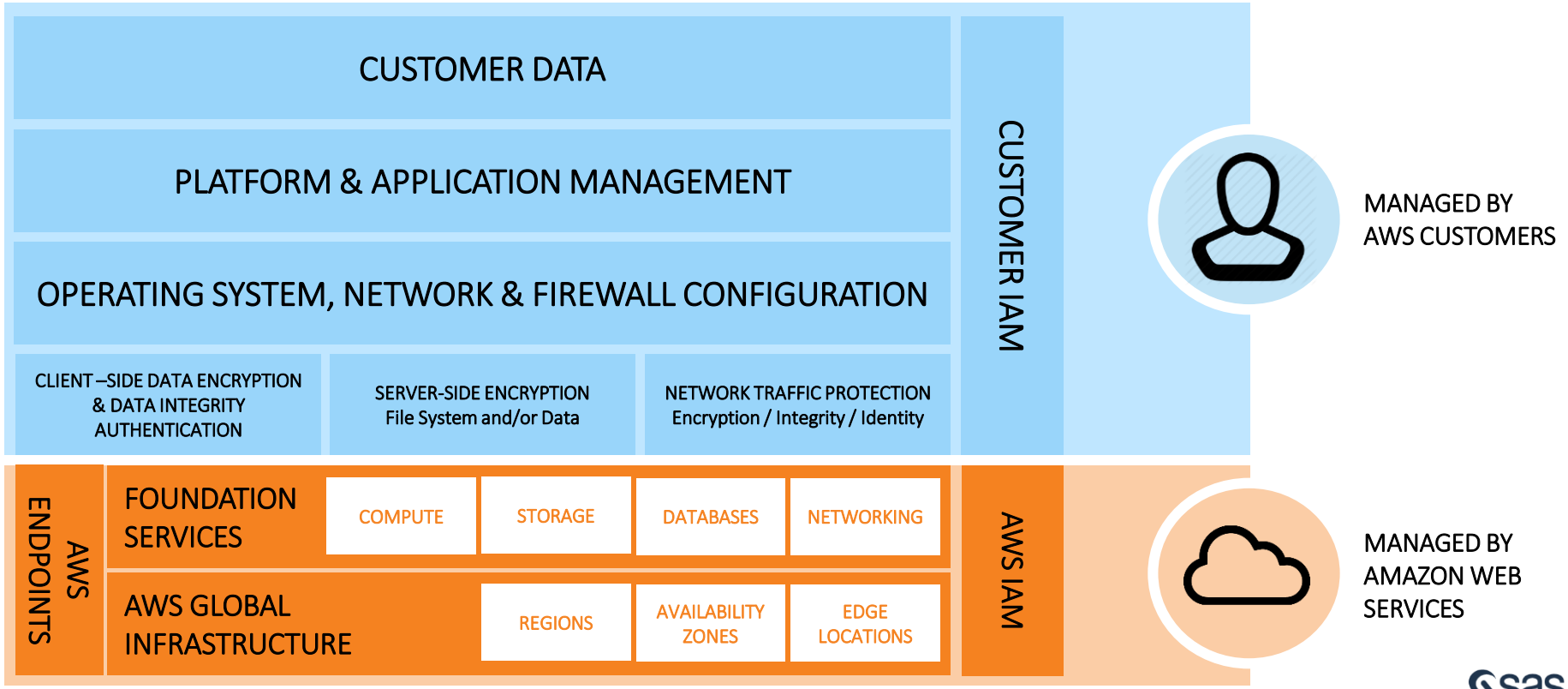
- Shared Security
  - Let the cloud provider do the heavy lifting
  - Focus on what's most valuable to your business

- Cloud Provider
  - Facilities
  - Physical security
  - Physical Infrastructure
  - Network infrastructure
  - Virtualization infrastructure
  - Hardware Lifecycle management

- Customer
  - Choice of Guest OS
  - Application Configuration
  - Account Management Flexibility
  - Security Groups
  - ACLs
  - Identity & Access Management
  - Data at rest & in transit

Shared Responsibility Model

Infrastructure Services



Grant Least Privilege

- Benefits
  - Less chance of people making mistakes
  - Easier to relax than tighten up
  - More granular control
    - API and resource
- How?
  - Identify what permissions are required
  - Password or access keys?
  - Don’t use *:* policies
  - Default Deny
  - Use policy templates

Manage Permissions

- Benefits
  - Easier to assign the same permissions to multiple users
  - Simpler to re-assign permissions if responsibilities change
  - Single change to update multiple users
- How?
  - Map permissions to a specific business function
  - Assign users to that function

Auditing

- Benefits
  - Visibility into user activity
  - e.g. AWS CloudTrail can record API calls to an S3 bucket
- How
  - Set up an Amazon S3 bucket
  - Enable AWS CloudTrail

Configure String Password Policy

- Benefit
  - Ensure users and data are protected
- How?
  - What's your company's password policy?
  - Configure
    - Password expiration
    - Password strength
      - Uppercase, lowercase, number etc
    - Password re-use

Enable MFS for privileged users

- Benefits
  - Supplements username and password to require a one-time code during authentication
- How?
  - Choose type
    - Virtual (e.g. smartphone)
    - Hardware
  - User IAM to assign MFS device

User IAM roles for instances

- Benefits
  - Easy to manage access keys on instances
  - Automatic key rotation
  - Assign least privilege to the application
- How?
  - Create an IAM role
  - Assign permissions to role
  - Launch instances with role

Remove use of root

- Benefits
  - Reduce potential for misuse of credentials
- How?
  - Security Credentials
    - Delete access keys
    - Activate MFA device
  - Ensure “strong” password set

Secure your data

At rest and in transit

- Benefits
  - Protect your data and customer information
  - Corporate / regulatory compliance
- How?
  - Storing and Managing encryption Keys
    - Store keys in tamper-proof storage
    - Hardware Security Modules
      - e.g. AWS CloudHSM
      - Store keys on-premise using your own HSMs and access over secure links
        - e.g. AWS Direct Connect or IPSec VPN over internet

Secure your Operating System and Applications

- Benefits
  - Reduce vulnerabilities
- How?
  - Standard OS hardening principles
    - e.g. CIS Benchmarks, DISA STIGs

Network Access Control Lists

- Benefits
  - Acts as a firewall for controlling traffic in and out of a subnet
  - Allow & Deny rules
- How?
  - e.g. AWS VPC
  - ! VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound traffic
  - Lock it down!

Direct Connect

- Benefits
  - Secure connection between Cloud and corporate network
  - Enables integration with corporate directory services (e.g. AD, LDAP etc)
- How?
  - Dedicated connection with hardware VPN

Considerations

- Bandwidth / Performance
  - Could appear slow moving large amounts of data into cloud
  - If moving large amounts of data in / out of cloud charges could be high
  - Increased latency of interactive applications e.g. Visual Analytics
  - May need high throughput instances (10Gbit interfaces)
- Backups
  - In-Cloud or corporate?
- Disaster Recovery
  - Automate everything
  - No need to have hardware sitting around doing nothing

Case Study #1

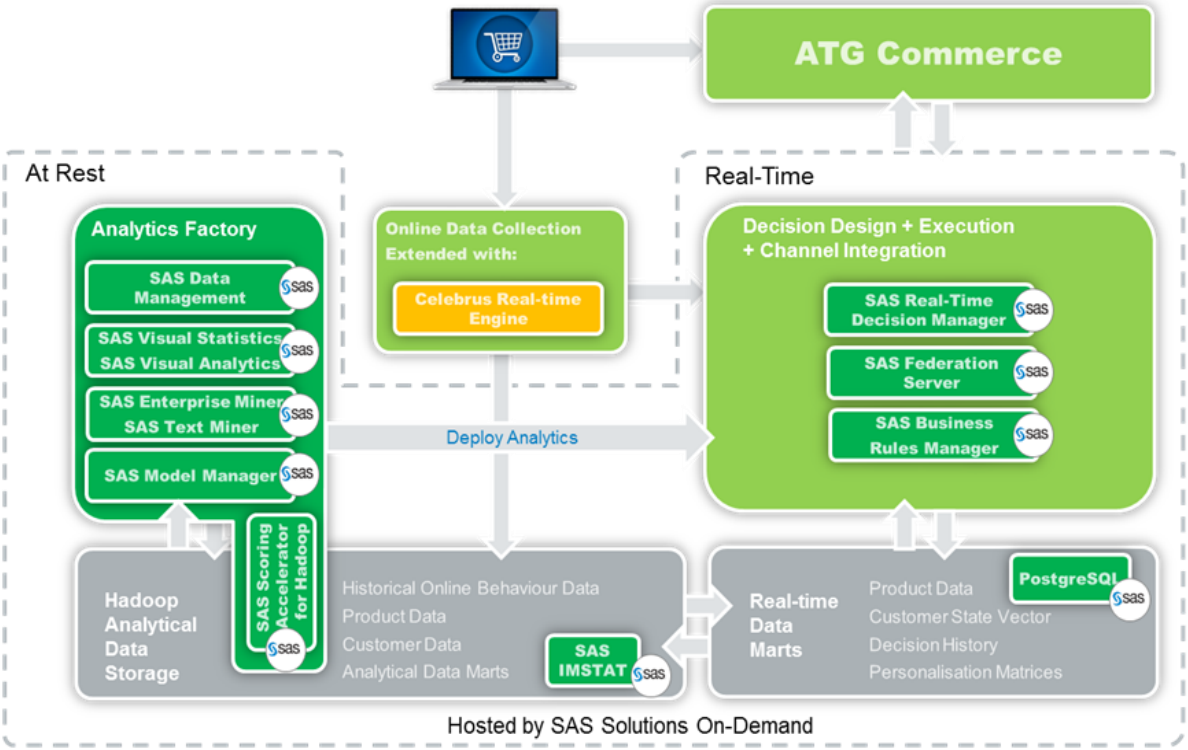
Medium Sized High Street Bank

- Analytics, IFRS9 and SAS Grid
- 300 Users
- Migrated from SAS 9.2 on premise solution
- AWS Production
  - 2 SAS GRID nodes (i2.8xlarge instances) 8x800GB SSD
  - 1 SAS GRID nodes (i2.xlarge instance) 1x800GB SSD
  - 1 SAS Metadata server (r3.4xlarge instance)
  - 1 SAS Midtier server. (r3.2xlarge instance)
- Intel Lustre Cloud Edition:
  - 1 Management server (MGS) (c4.4xlarge instance)
  - 1 Metadata server (MDS) (c4.8xlarge instance)
  - 2 Object Storage servers (OSS) (c4.8xlarge instances)
  - 2 Intel Lustre clients (c4.8xlarge instances) – just for backup-restore purpose
  - 1 DynamoDB instance for Intel Lustre configuration (50GB)
- Storage requirement:
  - 16 x 1 TB EBS (General Purpose SSD – gp2) volumes - every OSS server will have mounted 8 (eight) EBS (General Purpose SSD – gp2) volumes called OST , every volume will be size of 1 TB which will give us total of 16 TB shared file system space per site (single AZ) for SAS

Case Study #2

Large online fashion and household goods retailer

SOLUTION CAPABILITIES



Further Reading

- AWS Security Best Paractices
  - https://aws.amazon.com/blogs/security/new-whitepaper-aws-cloud-security-best-practices/
- Cloud Formation
  - https://aws.amazon.com/cloudformation/