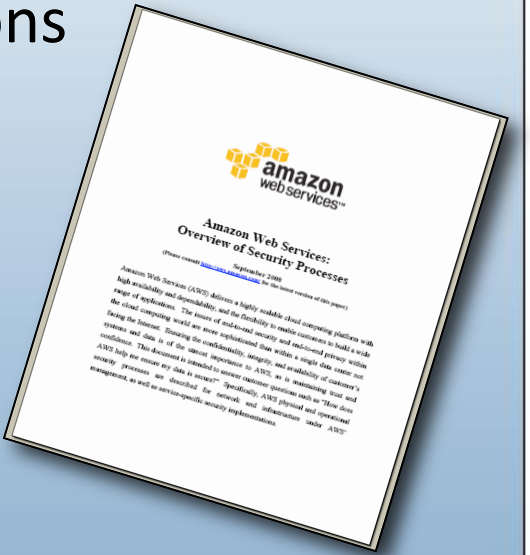
Fortress in the Cloud

Simone Brunozzi
Senior Technology Evangelist, AWS
Twitter: @simon

AWS Security and Compliance Center

(http://aws.amazon.com/security/)

- Answers to many security & privacy questions
  - Security whitepaper
  - Risk and Compliance whitepaper
- Security best practices
- Security bulletins
- Customer penetration testing
- More information on:
  - AWS Identity & Access Management (AWS IAM)
  - AWS Multi-Factor Authentication (AWS MFA)



amazon web services™

Amazon Web Services:
Overview of Security Processes

September 2008

(Please consult http://aws.amazon.com/ for the latest version of this paper)

Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and dependability, and the flexibility to enable customers to build a wide range of applications. The issues of end-to-end security and end-to-end privacy within the cloud computing world are more sophisticated than within a single data center not facing the Internet. Ensuring the confidentiality, integrity, and availability of customer's systems and data is of the utmost importance to AWS, as is maintaining trust and confidence. This document is intended to answer customer questions such as "How does AWS help me ensure my data is secure?" Specifically, AWS physical and operational security processes are described for network and infrastructure under AWS' management, as well as service-specific security implementations.

Shared Responsibility Model

AWS

- Facilities
- Physical Security
- Physical Infrastructure
- Network Infrastructure
- Virtualization Infrastructure

Customer

- Operating System
- Application
- Security Groups
- OS Firewalls
- Network Configuration
- Account Management

What does AWS do?

Physical Security of Data Centers

- Amazon has been building large-scale data centers for many years
- Important attributes:
  - Non-descript facilities
  - Robust perimeter controls
  - Strictly controlled physical access
  - 2 or more levels of two-factor auth
- Controlled, need-based access
- All access is logged and reviewed
- Separation of Duties
  - employees with physical access don’t have logical privileges

AWS Configuration Management

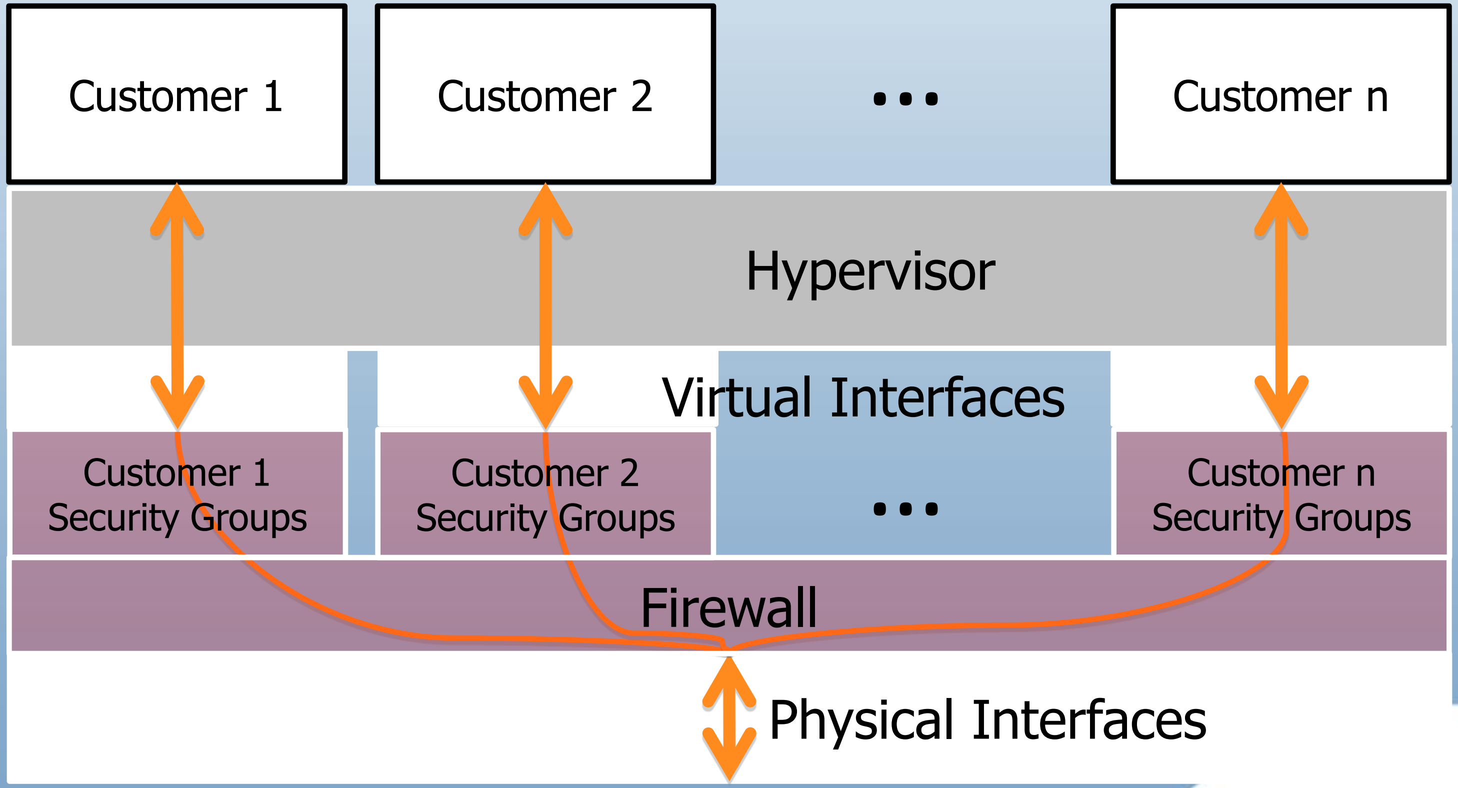
- Most updates are done in such a manner that they will not impact the customer
- Changes are authorized, logged, tested, approved, and documented
- AWS will communicate with customers, either via email, or through the AWS Service Health Dashboard (http://status.aws.amazon.com/) when there is a chance they may be affected

Customers are responsible for change control in their Instances!

EC2 Security

- Host operating system
  - Individual SSH keyed logins via bastion host for AWS admins
  - All accesses logged and audited
- Guest (a.k.a. Instance) operating system
  - Customer controlled (customer owns root/admin)
  - AWS admins cannot log in
  - Customer-generated keypairs
- Stateful firewall
  - Mandatory inbound firewall, default deny mode
  - Customer controls configuration via Security Groups
- Signed API calls
  - Require X.509 certificate or customer’s secret AWS key

Amazon EC2 Instance Isolation



Customer 1

Customer 2

...

Customer n

Hypervisor

Virtual Interfaces

Customer 1 Security Groups

Customer 2 Security Groups

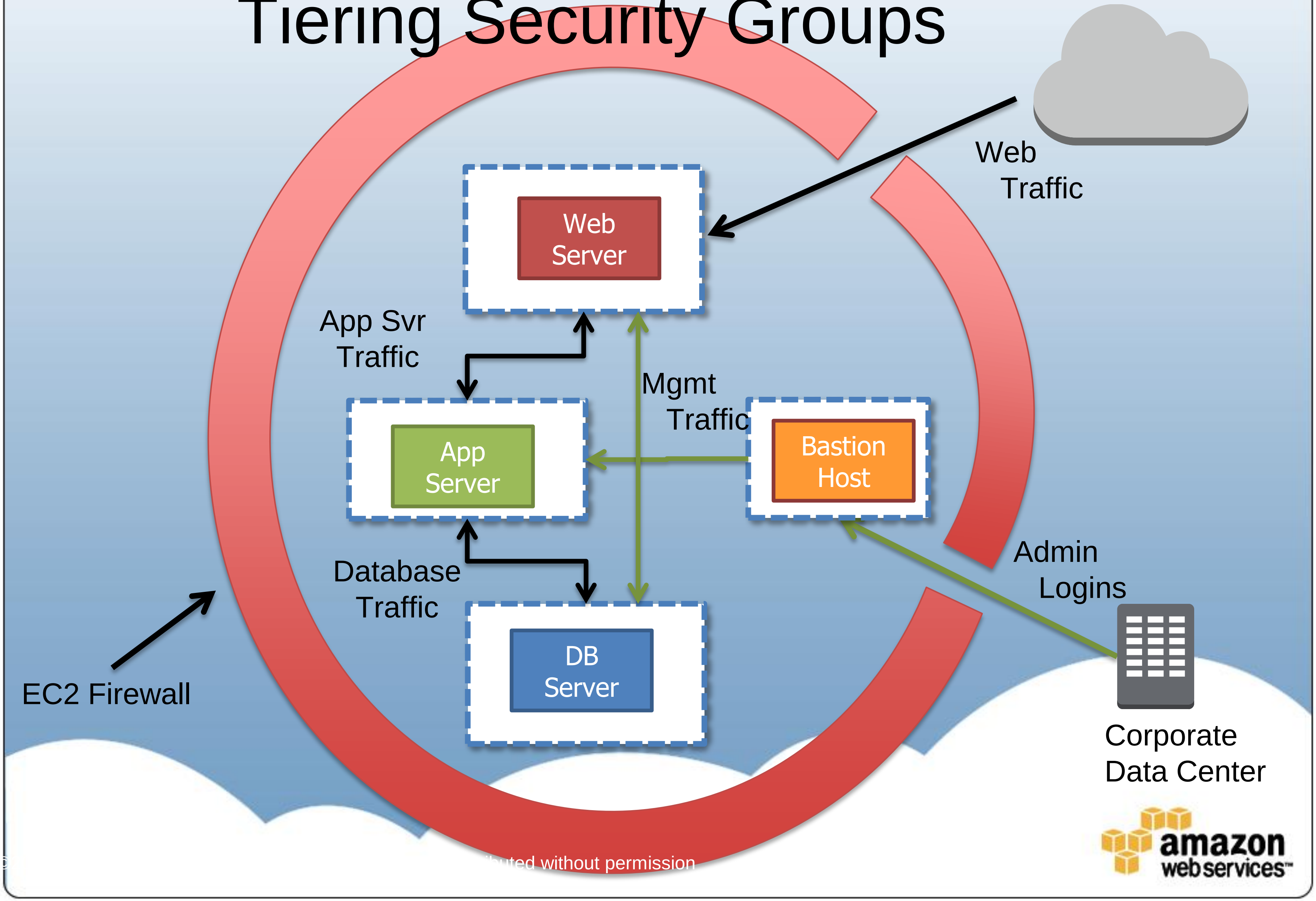
...

Customer n Security Groups

Firewall

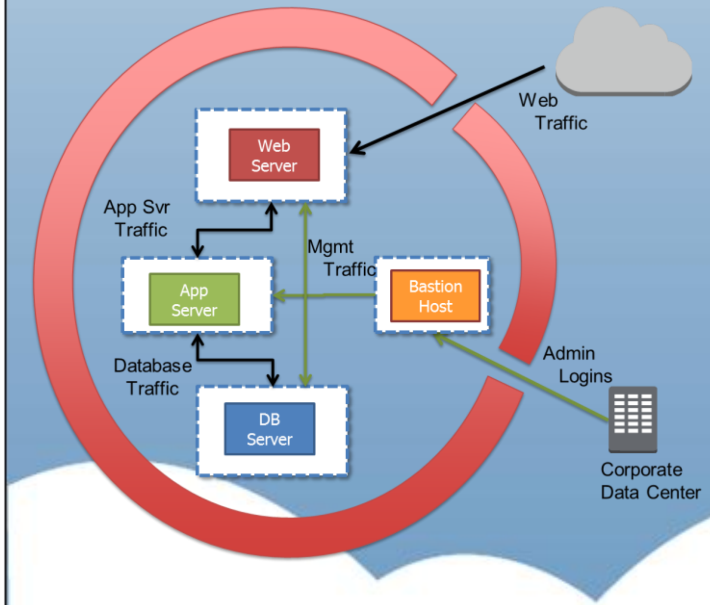
Physical Interfaces

Tiering Security Groups



Tiered EC2 Security Groups

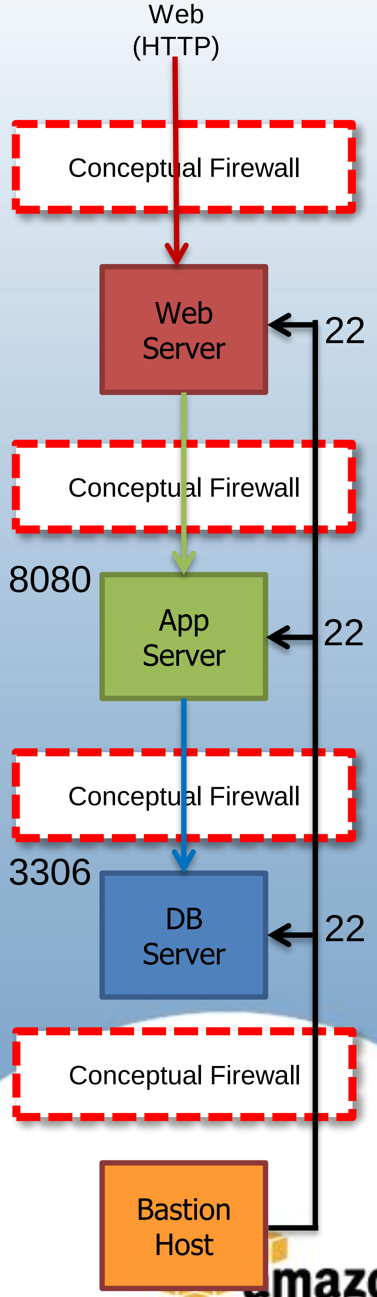
- Hierarchical Security Group Rules
  - Dynamically created rules
  - Based on Security Group membership
  - Create tiered network architectures



"Web" Security Group:
TCP 80 0.0.0.0/0
TCP 22 "Mgmt"
"App" Security Group:
TCP 8080 "Web"
TCP 22 "Mgmt"

"DB" Security Group:
TCP 3306 "App"
TCP 22 "Mgmt"

"Mgmt" Security Group:
TCP 22 163.128.25.32/32

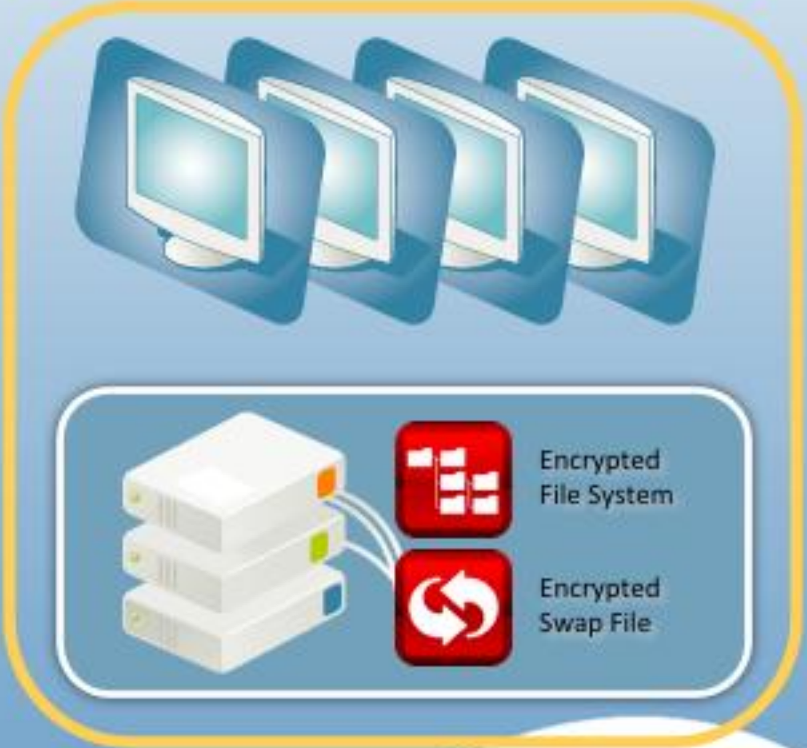


Network Security Considerations

- IP Spoofing:
  - Prohibited at host OS level
- Packet Sniffing:
  - Promiscuous mode is ineffective
  - Protection at hypervisor level
- Unauthorized Port Scanning:
  - Violation of AWS TOS
  - Detected, stopped, and blocked
  - Inbound ports blocked by default
- Distributed Denial of Service (DDoS):
  - Standard mitigation techniques in effect
- Man in the Middle (MITM):
  - All endpoints protected by SSL
  - Fresh EC2 host keys generated at boot

Virtual Memory & Local Disk

- Proprietary disk management prevents one Instance from reading the disk contents of another
- Disk is wiped upon creation
- Disks can be encrypted by the customer for an added layer of security



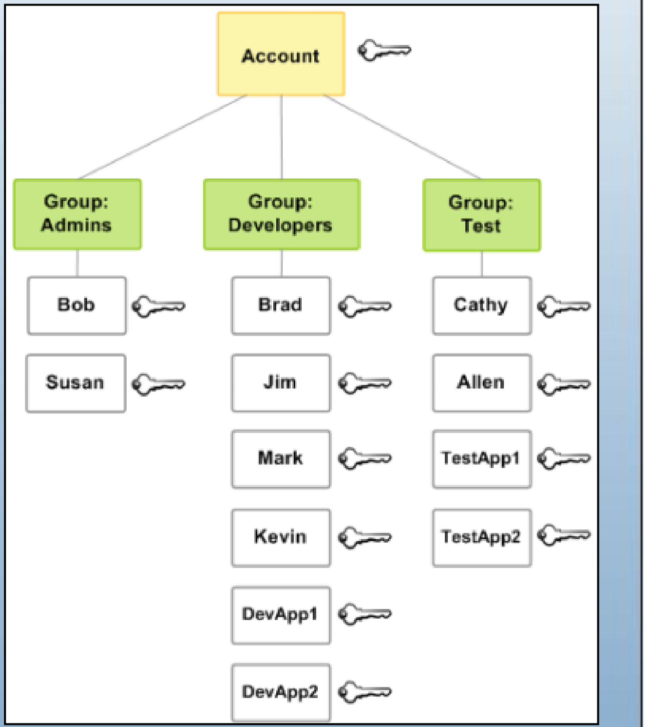
Storage Device Decommissioning

- All storage devices go through process
- Uses techniques from
  - DoD 5220.22-M (“National Industrial Security Program Operating Manual “)
  - NIST 800-88 (“Guidelines for Media Sanitization”)
- Ultimately
  - degaussed
  - physically destroyed

What tools does AWS provide to help build secure systems?

AWS Identity and Access Management (IAM)

- Users and Groups within Accounts
- Unique security credentials
  - Access keys
  - Login/Password
  - Enforce password complexity
  - optional MFA device
- Policies control access to AWS APIs
- API calls must be signed by either:
  - X.509 certificate
  - secret key
- Deep integration into some Services
  - S3: policies on objects and buckets
  - Simple DB: domains
- AWS Management Console supports User log on
- Not for Operating Systems or Applications
  - use LDAP, Active Directory/ADFS, etc...



AWS Multi-Factor Authentication

- Helps prevent anyone with unauthorized knowledge of your e-mail address and password from impersonating you
- Additional protection for account information
- Works with
  - Master Account
  - IAM Users
- Integrated into
  - AWS Management Console
  - Key pages on the AWS Portal
  - S3 (Secure Delete)

A recommended opt-in security feature!

AWS CloudHSM

- Secure Key Storage
  - Dedicated access to tamper-resistant HSM appliances (SafeNet® Luna SA)
  - Designed to comply with Common Criteria EAL4+ and NIST FIPS 140-2
  - You retain full control of your keys and cryptographic operations
- Contractual and Regulatory Compliance
  - Helps comply with the most stringent regulatory and contractual requirements for key protection.
- Reliable and Durable Key Storage
  - Available in multiple AZs and Regions
- Simple and Secure Connectivity
  - Connected to your VPC
  - Improved Application Performance between EC2 and HSM

Global Infrastructure for Global Companies

GovCloud (US ITAR Region)

US West (Northern California)

US West (Oregon)

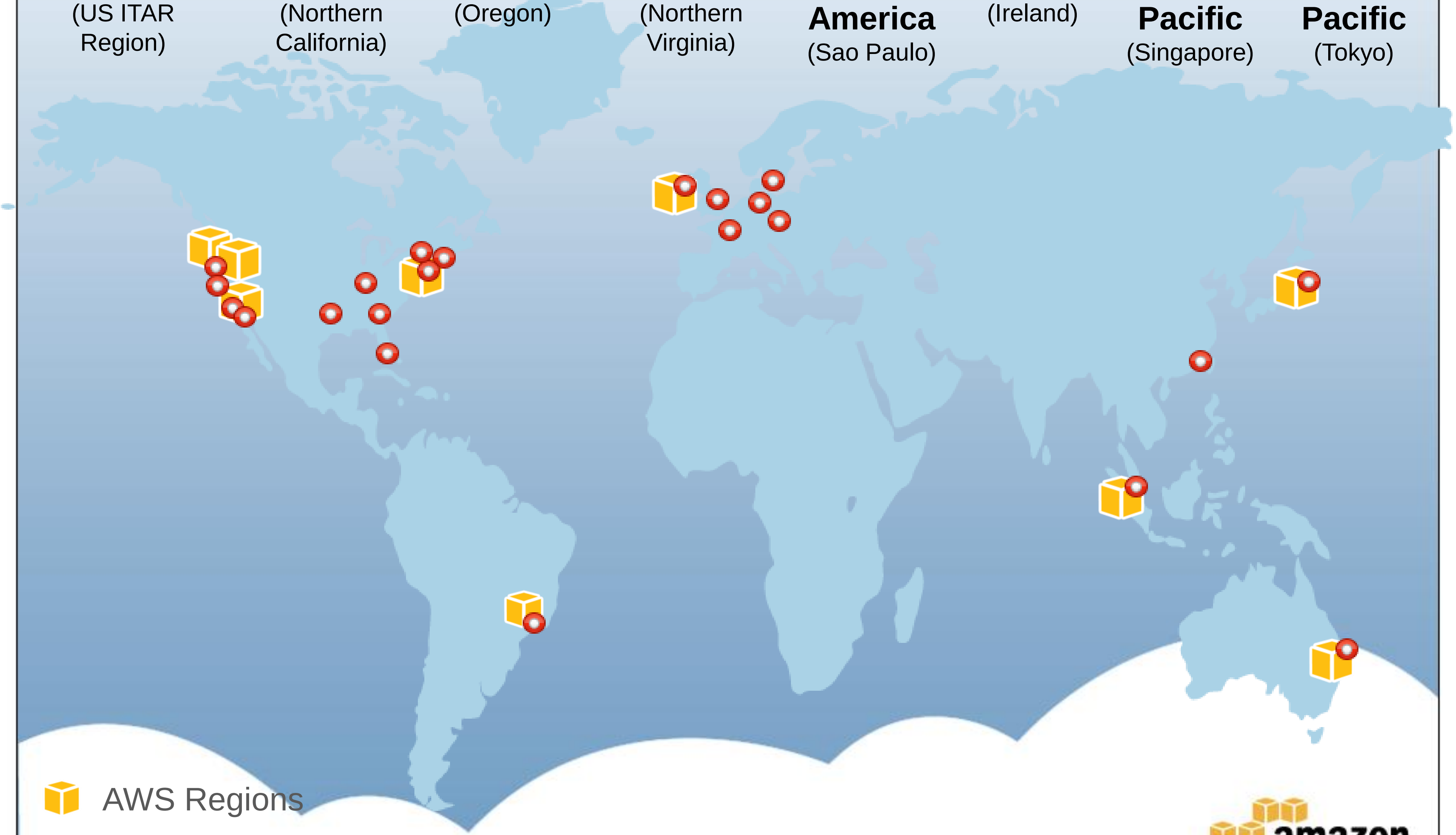
US East (Northern Virginia)

South America (Sao Paulo)

EU (Ireland)

Asia Pacific (Singapore)

Asia Pacific (Tokyo)

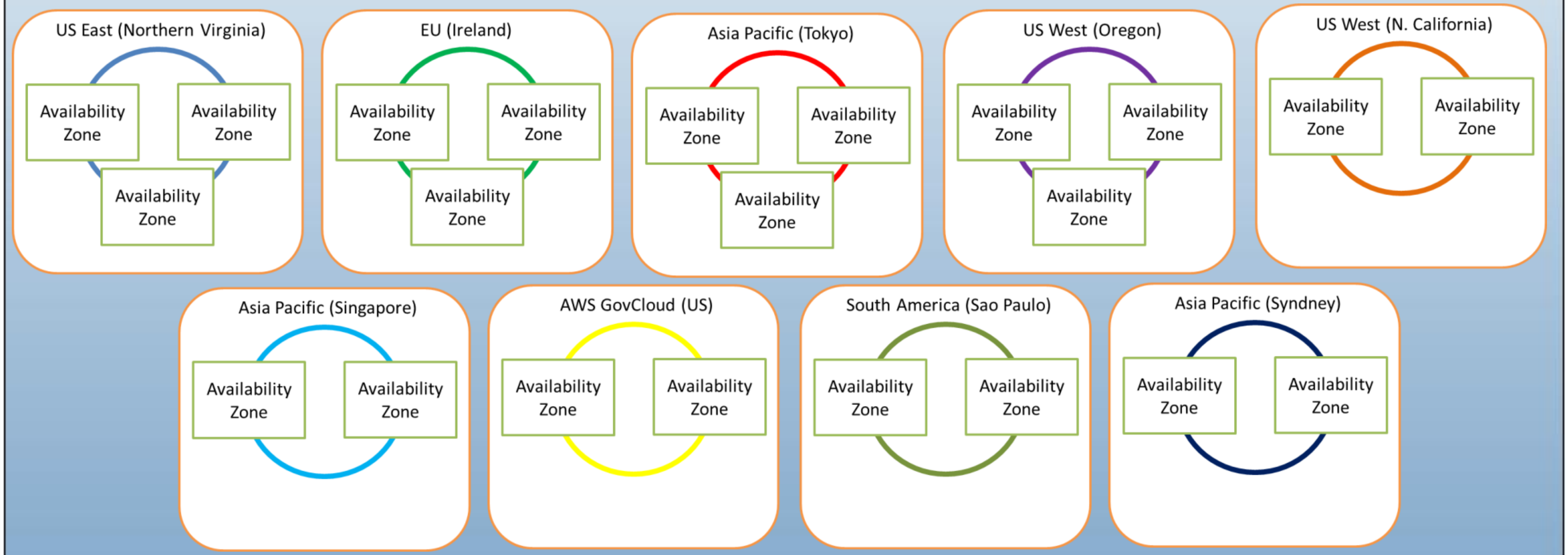


■ AWS Regions

● AWS Edge Locations

amazon webservices™

Amazon EC2 Regions and Availability Zones



Customers Decide Where Applications and Data Reside

amazon webservices™

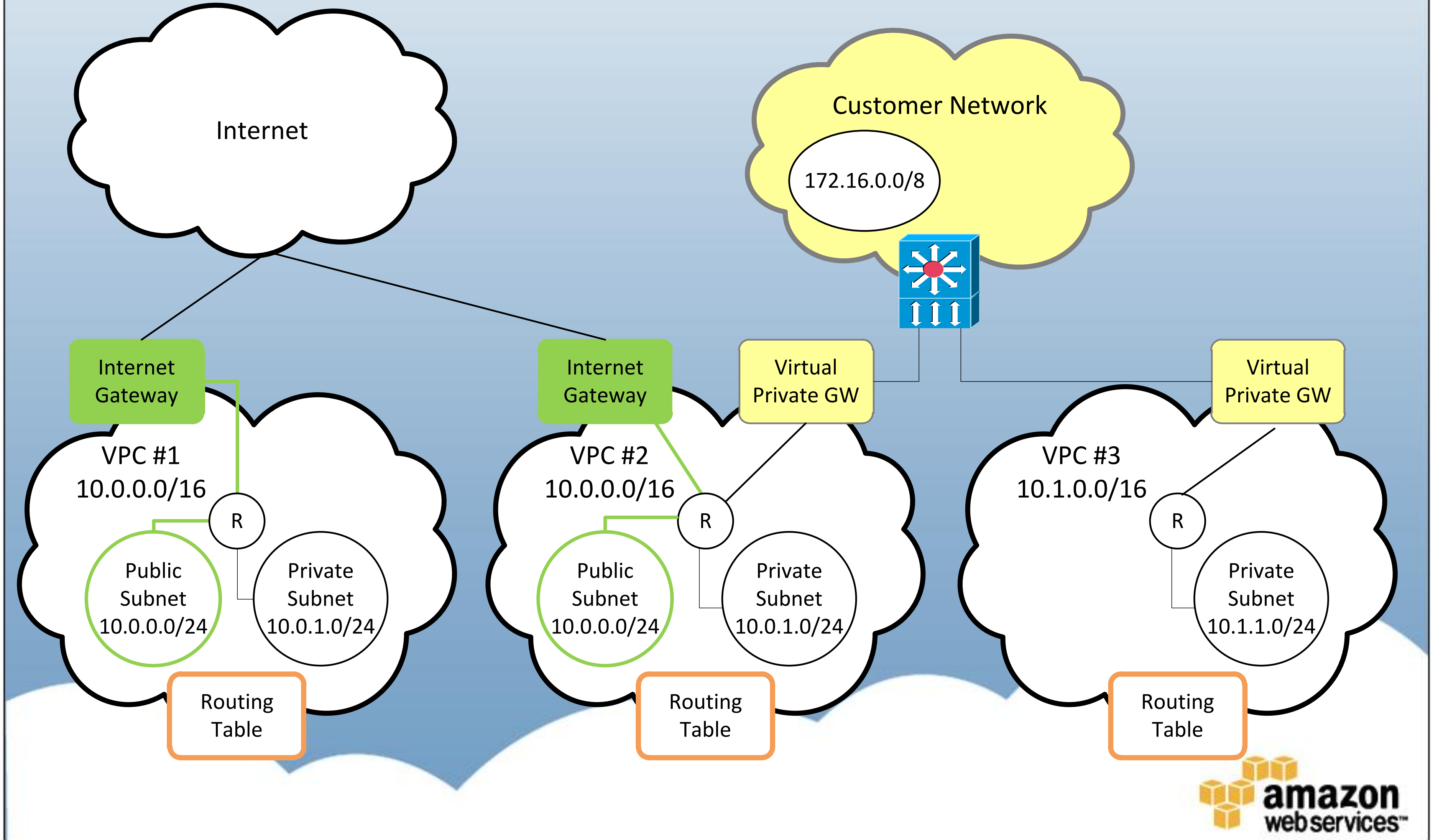
AWS is Built for "Continuous Availability"

- Scalable, fault tolerant services
- All Datacenters (AZs) are always on
  - No "Disaster Recovery Datacenter"
  - Managed to the same standards
- Robust Internet connectivity
  - Each AZ has redundant, Tier 1 ISP Service Providers
  - Resilient network infrastructure

Data Backups & Replication

- AWS favors replication over traditional backup
  - Equivalent to more traditional backup solutions
  - Higher data availability and throughput
  - No tapes with AWS customer data
- Makes data available in multiple edge locations
  - CloudFront, Route 53
- Data replicated to multiple Availability Zones within a single Region
  - S3, S3 RRS, DynamoDB, SimpleDB, SQS, RDS Multi-AZ, EBS Snapshots, etc…
- Data replicated to multiple physical locations within a single Availability Zone
  - EBS, RDS
- Data NOT automatically replicated
  - EC2 ephemeral drives (a.k.a. instance store)

Virtual Private Cloud

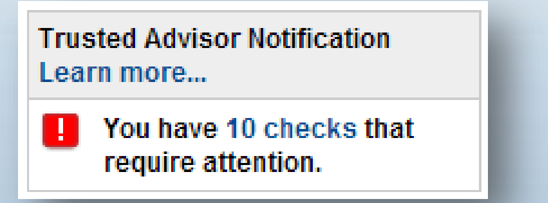


Customer Security Choices

- Flexible Networking Options
  - VPC vs. EC2 Classic
- EC2 Security Options
  - Choice of Operating System, hardening practices, security software
  - Customer controlled, customer-generated keypairs
  - Customer choice of security software, logging levels, and retention
  - Security Group configuration
  - Customer choice of hard drive encryption options
- S3 Security Options
  - ACLs and Bucket Policies
  - Server-side or client-side encryption

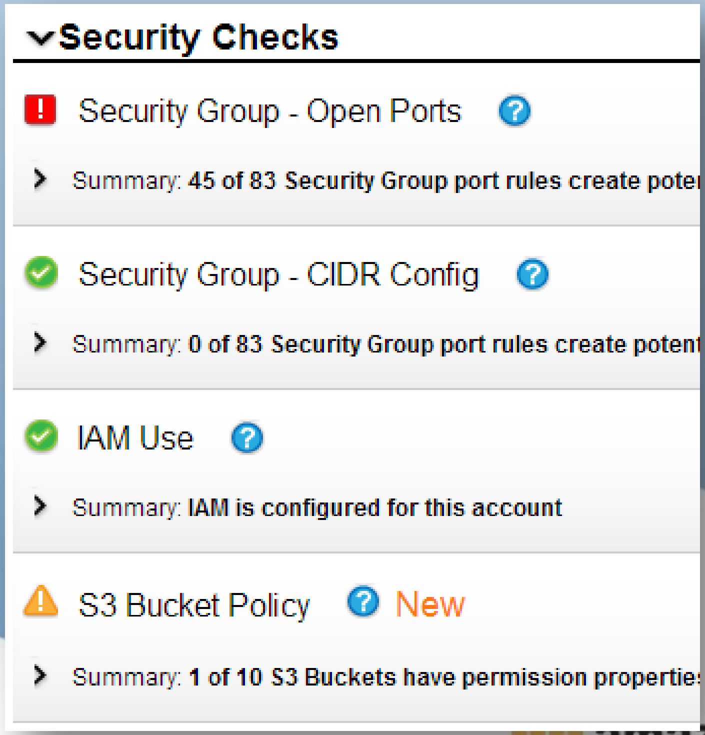
Premium Support - Trusted Advisor:

- Security Checks
  - Security Group Rules (Hosts & Ports)
  - IAM Use
  - S3 Policies
- Fault Tolerance Checks
  - Snapshots
  - Multi-AZ
  - VPN Tunnel Redundancy



Trusted Advisor Notification
Learn more...

! You have 10 checks that require attention.



Security Checks

! Security Group - Open Ports ?

› Summary: 45 of 83 Security Group port rules create pote

✓ Security Group - CIDR Config ?

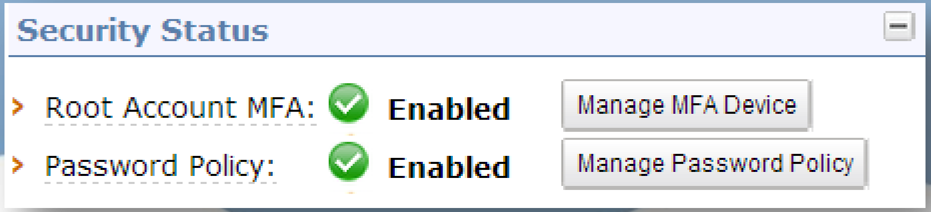
› Summary: 0 of 83 Security Group port rules create potent

✓ IAM Use ?

› Summary: IAM is configured for this account

⚠ S3 Bucket Policy ? New

› Summary: 1 of 10 S3 Buckets have permission propertie



Security Status

› Root Account MFA: ✓ Enabled [Manage MFA Device]

› Password Policy: ✓ Enabled [Manage Password Policy]

Some Additional Good Ideas:

- AWS is still the “real world”
- Least-Privilege design
- SOA design
- Classify resources and protect accordingly
- Security at every layer
- Inspect what you Expect

How can you be sure
(e.g. Who says so)?

AWS Certifications & Compliance

- AWS Environment
  - SOC 1, SOC 2, and SOC 3 Audits
  - ISO 27001 Certification
  - PCI DSS
  - FedRAMP (FISMA)
  - EU Data Protection 95/46/EC

- Customers have deployed various compliant applications:
  - Sarbanes-Oxley (SOX)
  - HIPAA (healthcare)
  - FISMA (US Federal Government)
  - DIACAP MAC III Sensitive ATO
  - International Traffic in Arms Regulations (ITAR)

Service Organization Controls

American Institute of Certified Public Accountants report

	What it contains	Who uses it
SOC 1	Attests that the AWS internal controls for financial reporting are appropriately designed and the controls are operating effectively	User auditors & users' controller's office. Shared under NDA by AWS.
SOC 2	Expanded evaluation of controls to include AICPA Trust Services Principles	Management, regulators & others. Shared under NDA by AWS.
SOC 3	Summary of SOC 2 and provides AICPA SysTrust Security Seal.	Management, regulators & others. Publicly available.

SOC 1

- Covers the majority of services in all regions
  - Control Objective 1: Security Organization
  - Control Objective 2: Amazon Employee Lifecycle
  - Control Objective 3: Logical Security
  - Control Objective 4: Secure Data Handling
  - Control Objective 5: Environmental Safeguards
  - Control Objective 6: Change Management
  - Control Objective 7: Data Integrity, Availability and Redundancy
  - Control Objective 8: Incident Handling
- Audited by an independent accounting firm and updated every 6 months
- Follows Statement on Standards for Attestation Engagements (SSAE) 16 format and International Standard on Assurance Engagements (ISAE) 3402 standards

SOC 2

- Follows AICPA Guide: Reporting on Controls at a Service Organizations Relevant to Security
- AICPA defined Trust Principles that cannot be omitted
- Additional granularity for specific services

Internal Control Components	Trust Principles of Security
• Control Environment	• Policies
• Risk Management	• Communications
• Information and Communication	• Procedures (Control Activities)
• Monitoring	• Monitoring
• Control Activities	

ISO 27001 Certification

- Covers the AWS Information Security Management System (ISMS)
- Follows ISO 27002 best practice guidance
- Includes all Regions
- Certification in the standard requires:
  - Systematic evaluation of information security risks
  - Evaluate the impact of company threats and vulnerabilities
  - Design and implement comprehensive information security controls
  - Adopt an overarching management process to ensure that the information security controls meet the information security needs on an ongoing basis

PCI DSS Level 1 Service Provider

- PCI DSS 2.0 compliant
- Covers core infrastructure & services
  - EC2, VPC, ELB, DirectConnect, S3, EBS, Glacier, RDS, DynamoDB, EMR, SimpleDB, and IAM
- Use normally, no special configuration
- Leverage the work of our QSA
- AWS will work with merchants and designated Qualified Incident Response Assessors (QIRA)
  - can support forensic investigations
- Certified in all regions

FedRAMP (FISMA) Moderate

- U.S. Civilian Government Agency Specific
- FedRAMP Approval To Operate (ATO)
- FISMA Moderate (NIST 800-53)
  - Much more stringent than other commercial standards
  - 205 high-level controls spanning 18 domains
    - Access Control, Awareness & Training, Audit & Accountability, Security Assessment & Authorization, Configuration Management, Contingency Planning, ID & Authentication, Incident Response, Maintenance, Media Protection, Physical & Environment Protection, Planning, Personnel Security, Risk Assessment, System & Services Acquisition, System & Communications Protections, System & Information Integrity, Program Management

Shared Assessments SIG

- Standard Information Gathering ("SIG") Questionnaire
  - www.sharedassessments.org
- Robust, easy to use set of questions to gather and assess
  - Information Technology
  - Operating and Security Risks (and corresponding controls)
- Based on referenced industry standards
  - Including, but not limited to, FFIEC, ISO, COBIT and PCI
- Excel format with AWS provided answers
- Updated periodically to stay current

Additional Initiatives

- Cloud Security Alliance (CSA) Questionnaire
  - Answers in the Risk and Compliance Whitepaper
- Motion Picture Association of America (MPAA)
  - Best practices for storing, processing and delivering protected media & content

AWS will Continue to Obtain Industry Certifications

- What other certifications matter to you?
- What is the impact to you?

Questions?

Thank You!

aws.amazon.com/security