Security:
A Driving Force Behind Moving to the Cloud

Michael South
Americas Regional Leader,
Public Sector Security & Compliance Business Acceleration

aws
Why is security traditionally so hard?

- Lack of Visibility
- Lack of Resiliency
- Defense in Depth
- Low degree of Automation
Four Security **Benefits** of the Cloud

- Increased *visibility*
- Increased *availability* and *resiliency*
- True **Defense-in-Depth**
- Ability to *automate* governance and Security Operations
Visibility
AWS Services that provide Operational Visibility

- **CloudTrail**: Track user activity and API usage
- **VPC Flow Logs**: Track network activity in/out of VPC
- **CloudWatch**: Monitor resources and applications
- **WAF Logs**: Track application access/denials
- **Inspector**: Analyze OS and application security
- **GuardDuty**: Intelligent Threat Detection
- **Trusted Advisor**: Guidance to reduce cost, increase performance, and improve security
- **Macie**: Discover, classify, and protect sensitive data
- **Artifact**: Self-service for AWS' compliance reports
Resiliency
18 Regions
55 Availability Zones
121 Edge Locations

Region & Number of Availability Zones

**AWS GovCloud**
- Oregon (3)
- Ohio (3) *Coming Soon*

**EU**
- Ireland (3)
- Frankfurt (3)
- London (3)
- Paris (3)

**US West**
- Oregon (3)
- Northern California (3)

**US East**
- N. Virginia (6)
- Seoul (2)
- Tokyo (4)
- Sydney (3)
- Mumbai (2)

**Canada**
- Central (2)

**South America**
- São Paulo (3)

**Announced Regions**
- Bahrain, Hong Kong, Sweden, AWS GovCloud East
- Regions: metropolitan area with independent “cloud”
- Fully Isolated from other Regions (security boundary)
  30 mile (appx) radius “clustered” data center architecture
- Customer chooses Region - Data Stays within Region
- Regions comprised of multiple Availability Zones
  AZ = 1 or more “data centers”
- AZ’s connected through redundant low-latency links
- Physically separated; Separate Low Risk Flood Plains
- Discrete UPS & Onsite backup
- Redundant connections to multiple tier-1 ISP’s
- Built for Continuous Availability
Achieving **High Availability** in AWS

Customer Datacenter

AWS Virtual Private Cloud (VPC)

AWS Region
Defense in Depth
Reality of Many On-Prem Network Defenses

Hard Outer Shell (Perimeter)
- WAF
- Firewall
- IDS/IPS
- DLP

Soft and Gooey Middle (Datacenter)
- VLANs
- ACLs
Defense-in-Depth in AWS at the Perimeter

AWS

VPC

VPC w/ ACLs
Stateless Firewall

172.16.0.0
172.16.1.0
172.16.2.0

VPN Gateway
Secure DevOps Comms

AWS Direct Connect
Private Fiber Comms

AWS Shield
DDoS Protection

AWS WAF
Web Application Firewall

Internet Gateway
Path to Public Internet
(Not present by default)

Amazon GuardDuty
Signature & Behavioral-based Intrusion Detection System using Machine Learning

DMZ Subnet

App Subnet

DB Subnet
Defense-in-Depth in **AWS** between **Workloads**

**VPCs w/ ACLs**
- Stateless Firewall
- Internet Gateway: Path to Public Internet
  - **VPN Gateway**
    - Secure Communications over Internet
- **VPN Peering**
  - Private network connection between VPCs

- **DMZ Subnet**
  - **Web Server**
  - **App Security Group**
- **App Subnet**
  - **App Server**
- **DB Subnet**
  - **DB Server primary**
  - **Database Security Group**

**Primary Subnets**
- 172.16.0.0
- 172.16.1.0
- 172.16.2.0

---

[Image of a network diagram showing VPCs with ACLs, DMZ, App, and DB subnets, and security groups with internet gateway and VPN gateway for secure communications.]
Defense-in-Depth in AWS inside the Workload

- **DMZ Subnet**
  - Web Server
  - Web Server
  - Web Server
  - DMZ Security Group

- **App Subnet**
  - App Server
  - App Server
  - App Server
  - App Security Group

- **DB Subnet**
  - DB Server primary
  - DB Server secondary
  - Database Security Group

- **Security Group**
  - Statefull Firewall between Each application tier

- **Security Group**
  - Does NOT allow peer-to-peer communications by default

- **Amazon GuardDuty**
  - Signature & Behavioral-based Intrusion Detection System using Machine Learning

- **Amazon CloudWatch**
  - Event Management and Alerting

- **AWS CloudTrail**
  - API Logging

- **3rd Party EPS**
  - OS Anti-virus, Firewall, Host Intrusion Protection System

- **Amazon Inspector**
  - Security & Compliance assessment
Amazon GuardDuty IDS

### Reconnaissance
- Instance recon:
  - Port probe / accepted comm
  - Port scan (intra-VPC)
  - Brute force attack (IP)
  - Drop point (IP)
  - Tor communications
  - Account recon
  - Tor API call (failed)

### Instance compromise
- C&C activity
- Malicious domain request
- EC2 on threat list
- Drop point IP
- Malicious comms (ASIS)
- Bitcoin mining
- Outbound DDoS
- Spambot activity
- Outbound SSH brute force
- Unusual network port
- Unusual traffic volume/direction
- Unusual DNS requests

### Account compromise
- Malicious API call (bad IP)
- Tor API call (accepted)
- CloudTrail disabled
- Password policy change
- Instance launch unusual
- Region activity unusual
- Suspicious console login
- Unusual ISP caller
- Mutating API calls (create, update, delete)
- High volume of describe calls
- Unusual IAM user added

- Detections in gray are signature based, state-less findings
- Detections in blue are behavioral, state-full findings / anomaly detections
Automate with integrated services

Automated threat remediation

GuardDuty → CloudWatch Events → Lambda → Web Application Firewall

Amazon GuardDuty → Amazon CloudWatch → CloudWatch Event → AWS Lambda → Lambda Function → AWS WAF → WAF Rule
# AWS security solutions

<table>
<thead>
<tr>
<th>Identity</th>
<th>Detective control</th>
<th>Infrastructure security</th>
<th>Data protection</th>
<th>Incident response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Identity &amp; Access Management (IAM)</td>
<td>AWS CloudTrail</td>
<td>Amazon EC2 Systems Manager</td>
<td>AWS Key Management Service (KMS)</td>
<td>AWS Config Rules</td>
</tr>
<tr>
<td>AWS Organizations</td>
<td>AWS Config</td>
<td>Systems Manager</td>
<td>AWS CloudHSM</td>
<td>AWS Lambda</td>
</tr>
<tr>
<td>AWS Cognito</td>
<td>Amazon CloudWatch</td>
<td>AWS Shield</td>
<td>Amazon Macie</td>
<td></td>
</tr>
<tr>
<td>AWS Directory Service</td>
<td>Amazon GuardDuty</td>
<td>AWS Web Application Firewall (WAF)</td>
<td>Certificate Manager</td>
<td></td>
</tr>
<tr>
<td>AWS Single Sign-On</td>
<td>VPC Flow Logs</td>
<td>Amazon Inspector</td>
<td>Server Side Encryption</td>
<td></td>
</tr>
</tbody>
</table>
Workloads appropriate for AWS

- Web applications and websites
- Backup, recovery, and archiving
- Disaster recovery
- Security Operations
- Development and test
- Data center migration and hybrid
- Mission critical applications
- Enterprise IT
- Big data
- High-performance computing
- Mobile
- IoT
Improving security with the cloud

“Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own datacenters.”

-Tom Soderstrom, CTO, NASA JPL

For more details, see Re:Invent 2013 presentations by NASA JPL cyber security engineer Matt Derenski (http://awsps.com/videos/SEC205E-640px.mp4)
The cloud is not only secure, but through shared responsibility, well-architected solutions, and best practices, it can be more secure than the traditional on-prem datacenter!
Thank you!

Questions?