Getting started with AWS security

Take a prescriptive approach

Stella Lee
Manager, Enterprise Business Development
$20B + Revenue Run Rate (Annualized from Q4 2017)

45% Y/Y Growth (Q4 2017 vs Q4 2016)
MILLIONS OF ACTIVE CUSTOMERS
GARTNER MAGIC QUADRANT FOR CLOUD INFRASTRUCTURE AS A SERVICE, WORLDWIDE
Amazon Innovation

Prime
One of the World’s Most Popular Subscription Services

Amazon Web Services
Our Cloud & Infrastructure Platform

Marketplace
Selling Products to Millions of Customers

Amazon Echo
A Device Designed Around Your Voice

Customer Reviews
Helping Customers Make Better Purchase Decisions

Amazon Fire TV
Tiny Box, Seamless Streaming

Prime Now
One-Hour Delivery for Prime Members

Amazon Launchpad
Today’s brightest startups, now on Amazon

Prime Air
Packages in 30 Minutes or Less

Dash Button
1-Click Ordering at Home

Amazon Fulfillment Network
Cutting Edge Technology, 50,000+ Employees

Amazon Kindle Reader
Revolutionizing the reading experience

Amazon Fresh
Grocery Delivery

Amazon Go
Advanced Shopping

Amazon Studios
Revolutionizing Music and Film
Why is enterprise security traditionally hard?

- Lack of visibility
- Low degree of automation
Making life easier

Choosing security does not mean giving up on convenience or introducing complexity.
Take a prescriptive approach to security

Understand AWS Security Approach

Build Strong Compliance Foundations

Integrate Identity and Access Management

Enable Detective Controls

Establish Network Security

Implement Data Protection

Optimize Change Management

Automate Security Functions
Understand how AWS practices security
SECURITY IS JOB ZERO
Security ownership is part of Amazon’s DNA

- Promotes culture of “everyone is an owner” for security
- Makes security a stakeholder in business success
- Enables easier and smoother communication
- Automates functions to reduce human access to near-zero
Moving to AWS can **strengthen** your security posture

- Over 30 global compliance certifications and accreditations
- Get native security functionality and tools
- Security infrastructure built to satisfy global banks and other high-sensitivity organizations
- Benefit from AWS industry leading security teams 24/7
- Leverage security enhancements gleaned from 1M+ customer experiences
Build On Strong Compliance Foundations
Get independent assurance from different sources

AWS Foundation Services

Compute  |  Storage  |  Database  |  Networking

AWS Global Infrastructure

Availability Zones  |  Regions  |  Edge Locations

AWS is responsible for the security of the Cloud

GxP  
ISO 13485  
AS9100  
ISO/TS 16949

AWS is responsible for the security of the Cloud
Customers control their own security policy

AWS is responsible for the security of the Cloud

Customers have their choice of security configurations **IN** the Cloud
Integrate Identity and Access Management
Control access with AWS Identity and Access Management

IAM Users
- Granular access control for least privileges
- Manage hierarchies of AWS Accounts with AWS Organizations
- Federate with your existing directory services

IAM Groups

IAM Roles
- Role-based access and segregation of duties
- Achieve just-in-time access using automation
- Create rich mobile applications without giving end-users long-term access keys

IAM Policies
Enable Detective Controls
AWS CloudTrail informs you of activity and Amazon CloudWatch alerts you when alarms go off

- Enable Globally for All AWS Regions
- Encryption and Integrity Validation of Log Files
- Archive and Forward
- Read by every industry-standard logging and SIEM platform

- Amazon CloudWatch Logs
- Metrics and Filters
- Alarms and Notifications
- Trigger automated actions
- Integrate with your existing ticketing systems
Establish Data Locality and Network Security
AWS Global Infrastructure

18 Regions – 54 Availability Zones – 113 Edge Locations

Region & Number of Availability Zones

AWS GovCloud (3)
EU
Ireland (3)

US West
Frankfurt (2)

US East
London (2)

Asia Pacific
Singapore (2)

Canada
Sydney (3)

South America
Tokyo (4), Osaka (1)*

Mumbai (2)

China
Beijing (2) Ningxia(2)

Announced Regions
Stockholm, HK, Bahrain, GovCloud(US-East)

Each region has at least two Availability Zones
You are in full control of privacy

Customers retain full ownership and control of their content

Choose an AWS Region and AWS will not replicate it elsewhere unless you choose to do so

Control format, accuracy and encryption any way that you choose

Control who can access content, it’s lifecycle and disposal

We publish GDPR resources on our website to help you meet your own compliance
Build your own isolated infrastructure with Amazon VPC

Amazon Virtual Private Cloud comes with granular security controls

Customer Premises

VPC fully supports IPv6
Internet access is **always** optional.

Everything not destined for my VPC goes to the Internet via the NAT Gateway.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.0/16</td>
<td>local</td>
<td>Active</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>NAT-Gateway ID012471</td>
<td>Active</td>
</tr>
</tbody>
</table>

Public IP: 54.2.0.12
VPC Flow Logs give you network insight

- Agentless
- From full VPC logging to a single NIC
- Logged to Amazon CloudWatch Logs so you can create alarms when metrics are breached
- Create your own network dashboards

<table>
<thead>
<tr>
<th>Interface</th>
<th>Source IP</th>
<th>Source port</th>
<th>Protocol</th>
<th>Packets</th>
<th>Start/end time</th>
<th>Accept or reject</th>
</tr>
</thead>
<tbody>
<tr>
<td>eni-b30b9cd5</td>
<td>119.147.115.32</td>
<td>10.1.1.179</td>
<td>6000</td>
<td>22</td>
<td>6 1 40 14429754735 1442975535</td>
<td>REJECT OK</td>
</tr>
<tr>
<td>eni-b30b9cd5</td>
<td>169.54.233.117</td>
<td>10.1.1.179</td>
<td>21188</td>
<td>80</td>
<td>6 1 40 1442975535</td>
<td>REJECT OK</td>
</tr>
<tr>
<td>eni-b30b9cd5</td>
<td>212.7.209.6</td>
<td>10.1.1.179</td>
<td>3389</td>
<td>3389</td>
<td>6 1 40 1442975596</td>
<td>REJECT OK</td>
</tr>
<tr>
<td>eni-b30b9cd5</td>
<td>189.134.227.225</td>
<td>10.1.1.179</td>
<td>39661</td>
<td>23</td>
<td>6 2 130 1442975656</td>
<td>REJECT OK</td>
</tr>
<tr>
<td>eni-b30b9cd5</td>
<td>77.85.113.238</td>
<td>10.1.1.179</td>
<td>0 1 100</td>
<td>1442975656</td>
<td>1442975716</td>
<td>REJECT OK</td>
</tr>
<tr>
<td>eni-b30b9cd5</td>
<td>10.1.1.179</td>
<td>198.60.73.8</td>
<td>512</td>
<td>123</td>
<td>17 1 76</td>
<td>1442975776</td>
</tr>
</tbody>
</table>
Block layer 7 attacks with AWS WAF

Now includes REGEX filtering!

Web traffic filtering with custom rules

Malicious request blocking

Active monitoring and tuning
Block DDoS attacks with AWS Shield

Advanced mitigation techniques

Deterministic filtering

Traffic prioritization based on scoring

Advanced routing policies
Implement Data Protection
AWS helps you encrypt everything, everywhere

AWS KMS
- Deep integration with AWS Services to make encryption simple
- Undergoing FIPS 140-2 validation
- Log and audit access with CloudTrail
- AWS SDK for easy integration
- Import your own encryption keys

Amazon CloudHSM
- Cloud-based Hardware Security Modules (HSMs)
- FIPS 140-2 Level 3 validated
- Integrate with on-premises HSMs
- Industry standard cryptographic APIs
Make every website HTTPS with Amazon Certificate Manager

Everyone is moving to HTTPS so make it easy for yourself and remove the manual process

- Easily provision, manage and deploy TLS/SSL certificates to AWS
- Supports API Gateway, Cloudfront CDN and Elastic Load Balancer
- AWS Certificate Manager handles certificate renewals for you
- Provisioned certificates are free
Amazon Macie will classify and track your data.

MACHINE LEARNING SERVICE TO HELP CUSTOMERS PREVENT DATA LOSS IN AWS.
When access to data changes, Macie will tell you

- PII and PHI
- Static website content
- Source code
- SSL certificates, private keys
- iOS and Android app signing keys
- Database backups
- OAuth and Cloud SAAS API Keys
Optimize Change Management
AWS Config tracks **changes** to your resources and Config Rules **assesses** them against security policy.

**AWS Config**
- Record configuration changes continuously
- Time-series view of resource changes
- Archive and compare

**Config Rules**
- Assess changes against your security policy
- Enforce best practices
- Automatically roll back unwanted changes
- Trigger additional workflow
Automate Security Functions
Trusted Advisor automates governance

Remember when reports were done manually?
AWS CloudFormation automates infrastructure as code

- Orchestrate changes across AWS Services
- Use as foundation to Service Catalog products
- Use with source code repositories to manage infrastructure changes

**Template**
- JSON-based text file describing infrastructure

**Stack**
- Resources created from a template can be updated
- Updates can be restricted
You can evolve the practice of security architecture

Security architecture should not be a separate function!

Current Security Architecture Practice

Static position papers, architecture diagrams, and documents

UI-dependent consoles and technologies

Auditing, assurance, and compliance are decoupled, separate processes
Your architecture defines your operations

Security becomes a core part of the ’maker’ team

Evolved Security Architecture Practice

Architecture artifacts (design choices, narrative, etc.) committed to common repositories

Complete solutions account for automation

Solution architectures are living audit/compliance artifacts and evidence in a closed loop

AWS CodeCommit

AWS CodePipeline

Jenkins
A prescriptive approach to cloud security – get started!

Understand AWS Security Approach

Build Strong Compliance Foundations

Integrate Identity and Access Management

Enable Detective Controls

Establish Network Security

Implement Data Protection

Optimize Change Management

Automate Security Functions
Thank You!