ServerlessToronto.org Meetup Agenda

Thursday, Apr 18, 2019

PURESEC

1. Intro & Activity Update
2. Community Open Mic

3. Andrew Brown, ExamPro: "Serverless Security in AWS Cloud"
4. Mike Apted, AWS Canada: "Serverless, Startups & AWS - The beginning of a beautiful friendship"

myplanet

5. Networking

MANNING PUBLICATIONS

Manning Publications 2019 giveaways:

1. www.manning.com/books/serverless-applications-with-nodejs
2. www.manning.com/livevideo/production-ready-serverless
3. ~~www.manning.com/livevideo/production-ready-serverless~~
4. www.manning.com/livevideo/serverless-applications-with-AWS
5. www.manning.com/livevideo/serverless-applications-with-AWS
6. www.manning.com/books/serverless-architectures-on-aws
7. www.manning.com/books/http2-in-action
8. ~~www.manning.com/books/event-streams-in-action~~
9. www.manning.com/books/the-design-of-everyday-apis
10. www.manning.com/livevideo/graphql-in-motion
11. www.manning.com/books/voice-applications-for-alexa-and-google-assistant
12. www.manning.com/livevideo/machine-learning-for-mere-mortals
13. ~~www.manning.com/books/classic-computer-science-problems-in-python~~

serverless user group

Shared Model of Responsibility

APPLICATION OWNER

RESPONSIBLE FOR SECURITY "IN" THE CLOUD

CLIENT-SIDE | DATA IN CLOUD | DATA IN TRANSIT

APPLICATIONS (FUNCTIONS)

IDENTITY & ACCESS MANAGEMENT | CLOUD SERVICES CONFIGURATION

CLOUD PROVIDER

RESPONSIBLE FOR SECURITY "OF" THE CLOUD

OPERATING SYSTEM + VIRTUAL MACHINES + CONTAINERS

COMPUTE | STORAGE | DATABASE | NETWORK

REGIONS | AVAILABILITY ZONES | EDGE LOCATIONS

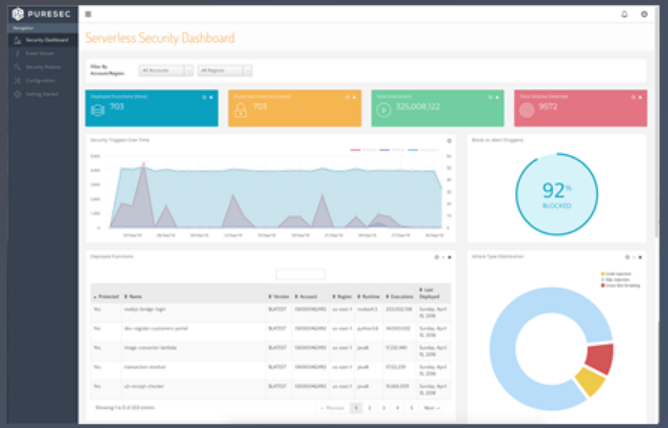
Puresec SSP: The Leading End To End Protection For Serverless

SERVERLESS POSTURE MANAGEMENT

- SERVERLESS ASSET INVENTORY
- VULNERABILITY MANAGEMENT
- DETECT IAM & CONFIGURATION ISSUES
- CI / CD INTEGRATION

RUNTIME PROTECTION

- SERVERLESS APPLICATION FIREWALL
- BEHAVIORAL PROTECTION W/ ML
- BLAZING FAST
- PAINLESS DEPLOYMENT



SECURITY VISIBILITY

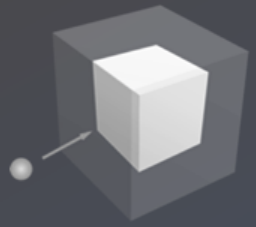
- REAL TIME APP SECURITY VISIBLITY
- DEEP FORENSIC ANALYSIS
- SIEM INTEGRATIONS

Security Posture Management

During CI/CD

Code & configuration analysis to detect & mitigate known vulnerabilities

Static Analysis



When Invoked

Controls the perimeter of each function in order to prevent malicious input from entering

Serverless App Firewall

During Execution

Controls function behavior in order to ensure it works as intended

Behavioral Protection

Deep Visibility

Community Open Mic

serverless
user group

Exam Pro

Launch Talk

April 18 2019

Andrew Brown

andrew@exampro.co

CEO of ExamPro
12 Year Full Stack Developer
4/10 AWS Certifications
Loves StarTrek DS9

Full-Stack ⚡ Powerleveling

The Fast Track to Serverless Security on AWS

This Tech Talk Is Designed To Help You Study For The Security Speciality AWS Certification

Param Store, Secrets Manager		Keeping our secrets a secret
CloudFront, AWS Shield		Mitigating DDoS Attacks
KMS - Key Management Service		Encrypting data at rest
ACM - AWS Certification Manager		Encrypting data in transit
IAM - Identity and Access Management		Least permissive IAM policies
Lambda		Securing AWS Lambda Functions
WAF - Web Application Firewall		Protect against common exploits and attacks
Macie, Guard Duty		Automated Security with ML services

Serverless Security Resources

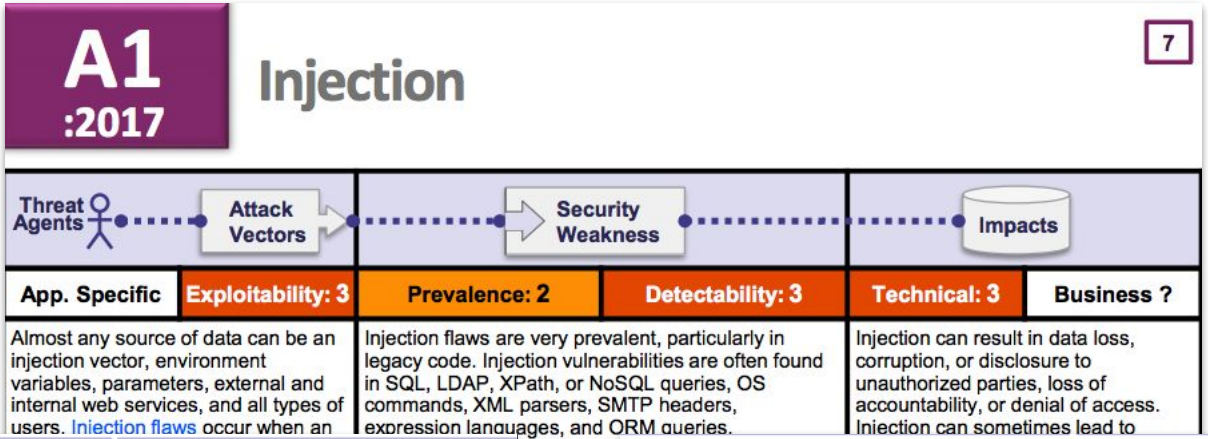
OWASP

Open Web Application Security Project

Serverless Security Resources

1. Injection
2. Broken Authentication and Session Management
3. Sensitive Data Exposure
4. XML External Entity
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure deserialization
9. Using Components With Known Vulnerabilities
10. Insufficient Logging and Monitoring

Serverless Security Resources



Is the Application Vulnerable?

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures.

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections, closely followed by thorough automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs. Organizations can include static source (SAST) and dynamic application test (DAST) tools into the CI/CD pipeline to identify newly introduced injection flaws prior to production deployment.

How to Prevent

Preventing injection requires keeping data separate from commands and queries.

- The preferred option is to use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs).
  Note: Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec().
- Use positive or "whitelist" server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
- For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter.
  Note: SQL structure such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software.
- Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.

Example Attack Scenarios

Scenario #1: An application uses untrusted data in the construction of the following vulnerable SQL call:

```
String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";
```

Scenario #2: Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g. Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts WHERE custID='" + request.getParameter("id") + "'");
```

In both cases, the attacker modifies the 'id' parameter value in their browser to send: **' or '1'='1**. For example:

```
http://example.com/app/accountView?id=' or '1'='1
```

This changes the meaning of both queries to return all the records from the accounts table. More dangerous attacks could modify or delete data, or even invoke stored procedures.

References

OWASP

- OWASP Proactive Controls: Parameterize Queries
- OWASP ASVS: V5 Input Validation and Encoding
- OWASP Testing Guide: SQL Injection, Command Injection, ORM injection
- OWASP Cheat Sheet: Injection Prevention
- OWASP Cheat Sheet: SQL Injection Prevention
- OWASP Cheat Sheet: Injection Prevention in Java
- OWASP Cheat Sheet: Query Parameterization
- OWASP Automated Threats to Web Applications – OAT-014

External

- CWE-77: Command Injection
- CWE-89: SQL Injection
- CWE-564: Hibernate Injection
- CWE-917: Expression Language Injection
- PortSwigger: Server-side template injection

KMS - Key Management Service

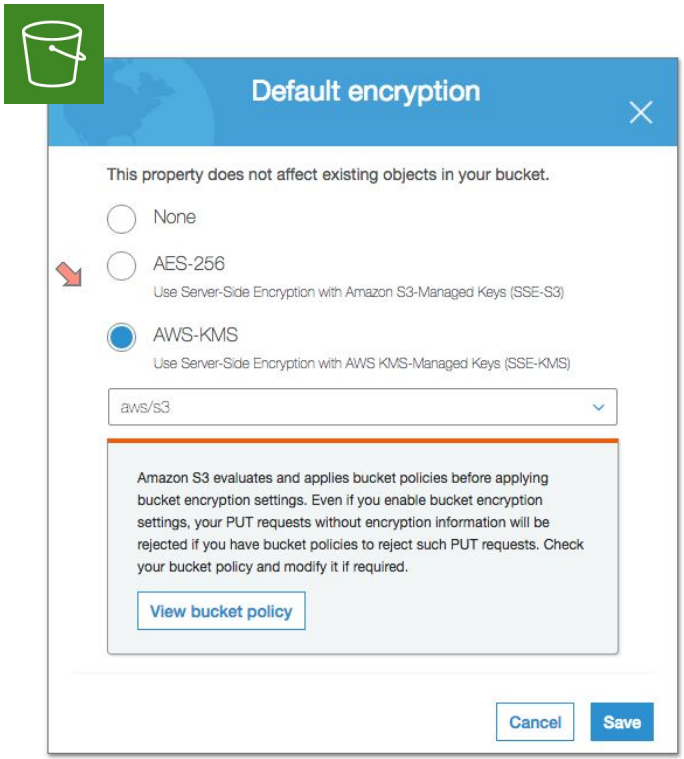
$1 / per key

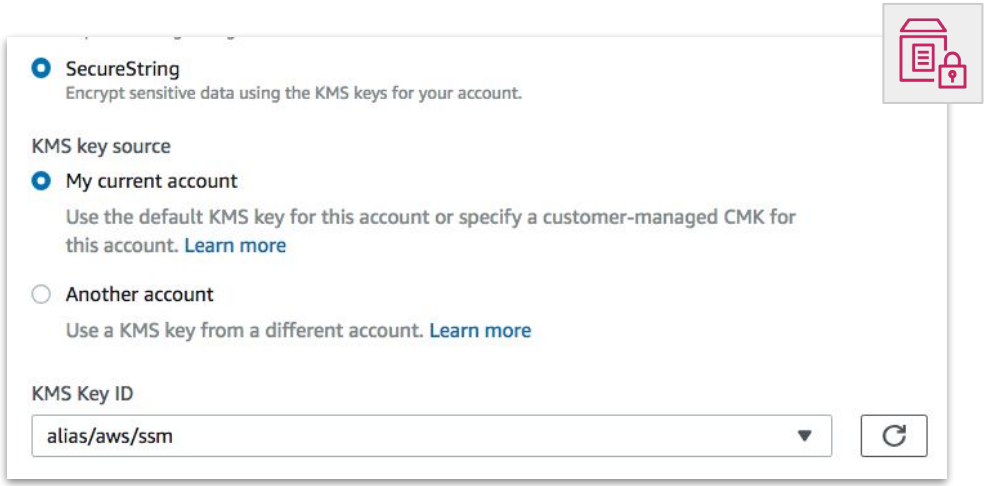
checkbox secure ☑ and start encrypting

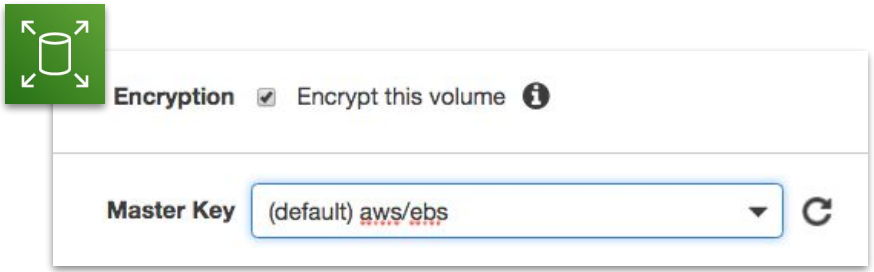
Multi-tenant HSM to create and control encryption keys

HARDWARE SECURITY MODULE

KMS integrates with many AWS services







Securing AWS Lambda Functions

lets you run code without provisioning or managing servers

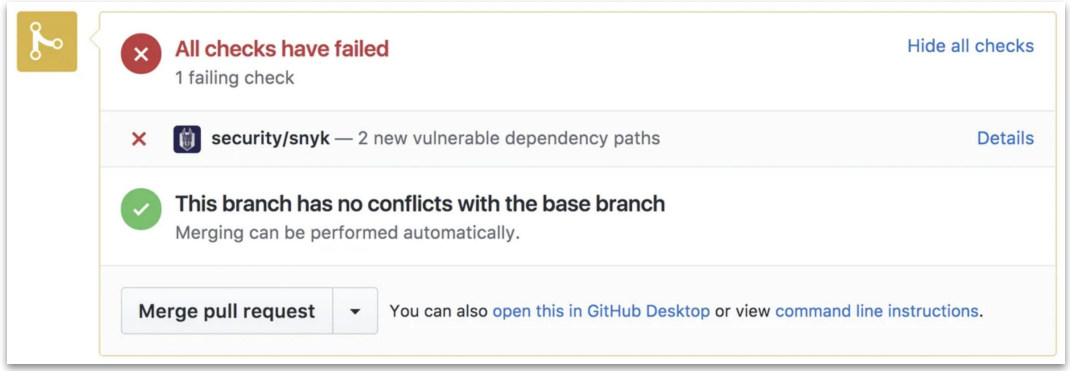
- Scan vulnerabilities in your 3rd party dependencies
- Prevent event-data injection
- Least permissive IAM policies
- Keeping our secrets a secret
- Lambda Protection from AWS Lambda Partners
- Lambda Compliance

Securing AWS Lambda Functions

Scan vulnerabilities in your 3rd party dependencies

Snyk

A developer-first solution that automates finding & fixing vulnerabilities in your dependencies



Securing AWS Lambda Functions

Prevent Event-Data Injection

File name
"DELETE * FROM USERS"

Securing AWS Lambda Functions

Least Permissive IAM Policies

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3 Permissions",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
    ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3 Permissions",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:ListBuckets"
      ],
    ]
}
```

Securing AWS Lambda Functions

Keeping Our Secrets a Secret

SSM Param Store

- Free!
- Versioned
- Rotate Keys with Cloudwatch + Lambda

Secrets Manager

$$$ - $0.40 /secret

- RDS Integration
- Multiple Key / Values in on Secret
- *Automated Key Rotation (via Lambda)
- Restore Accidentally deleted secrets

Stores sensitive data such as passwords

AWS Lambda Compliance

Compliant with:

- SOC 1
- SOC 2
- SOC 3
- PCI DSS
- HIPAA

Use **AWS Artifact** to gain access to these reports on how AWS is compliant

GaurdDuty

DNS and Flow Logs

Macie

CloudTrail Logs for S3

Both use **machine learning** to **analyze logs**

GuardDuty
Findings
Settings
Lists
Accounts
What's New
Usage
Partners

New feature: New Root Credential Detection
Amazon GuardDuty has added a new finding type that notifies you when root credentials are used programatically in your account. Learn more

Findings

Showing 33 of 33 — 33 | 0 | 0

Actions | Saved filters / Auto-archive: No saved filters

Current | Add filter criteria

Finding type	Resource	Last s...	Co...
Recon:EC2/PortProbeUnprotected...	Instance: i-05e8996590e85b1b3	a mon...	280
Recon:EC2/PortProbeUnprotected...	Instance: i-0d89ad53f4d6f3f94	a mon...	330
Recon:EC2/PortProbeUnprotected...	Instance: i-04fae5b8df570e6ce	a mon...	310
Recon:EC2/PortProbeUnprotected...	Instance: i-0269e117c812c22fd	a mon...	253
UnauthorizedAccess:EC2/SSHBrut...	Instance: i-0269e117c812c22fd	a mon...	1
UnauthorizedAccess:EC2/SSHBrut...	Instance: i-04fae5b8df570e6ce	a mon...	1
UnauthorizedAccess:EC2/SSHBrut...	Instance: i-0269e117c812c22fd	a mon...	1
UnauthorizedAccess:EC2/SSHBrut...	Instance: i-04fae5b8df570e6ce	a mon...	2
UnauthorizedAccess:EC2/SSHBrut...	Instance: i-05e8996590e85b1b3	a mon...	35
UnauthorizedAccess:EC2/SSHBrut...	Instance: i-05e8996590e85b1b3	a mon...	5

Useful? Close

UnauthorizedAccess:EC2/SSHBruteForce

Finding ID: 8ab43ae3b9a5cf5c032aab5f0914a468

76.72.169.18 is performing SSH brute force attacks against i-04fae5b8df570e6ce. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.

Severity	Region	Count
Low	us-east-1	1
Account ID	**Resource ID**	**Created at**
655604346524	i-04fae5b8df570e...	01-22-2019 08:37...
Updated at		
01-22-2019 08:37...		

Resource affected

Resource role	Resource type
TARGET	Instance
Instance ID	**Port**
i-04fae5b8df570e6ce	22
Port name	**Instance type**
SSH	t2.small
Instance state	**Availability zone**
running	us-east-1a
Image ID	**Image description**
ami-06aa276f0e7597475	Agent Installed, Bundle
Launch time	

List management

Trusted IP lists

Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more

Add a trusted IP list

List name	List file URL	Format	Active

Trusted IP lists
Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more

Threat lists

Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more

Add a threat list

List name	List file URL	Format	Active

Threat lists
Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more

Macie

root US East (N. Virginia)

- DASHBOARD
- ALERTS
- USERS
- RESEARCH
- SETTINGS
- INTEGRATIONS

Critical assets
(0% of all)

N/A
High risk (levels 8, 9, and 10)

Total event occurrences

N/A
Number of event occurrences

Total user sessions

N/A
Number of user sessions

Platinum: This IAM user or role has a history of making high risk API calls and should be monitored closely for signs of account compromise.

0 0 0 0

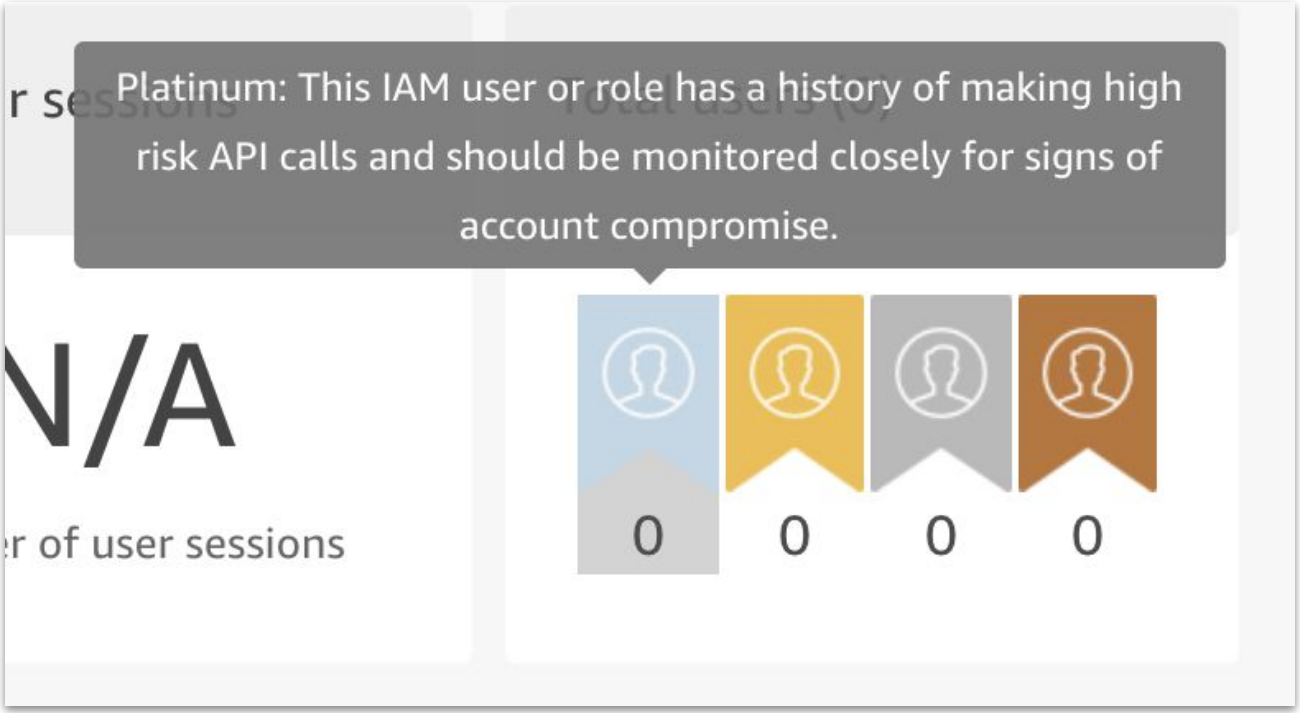
Minimum risk: 5

Move the slider to only view items at or above the selected risk level.

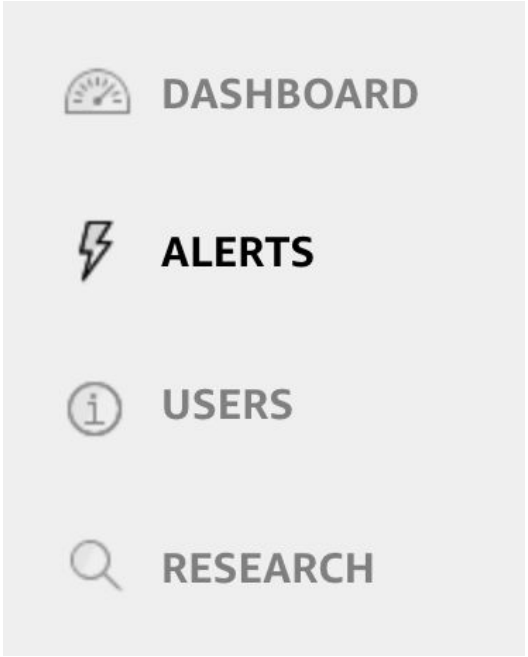
S3 objects for selected time range - minRisk: (5)

The following graph shows S3 objects grouped into top 20 matching themes for the selected time range. To further investigate your S3 objects, double-click sections of the graph or color chart. **Learn more**

Macie


Platinum: This IAM user or role has a history of making high risk API calls and should be monitored closely for signs of account compromise.
N/A
r of user sessions
0
0
0
0

Macie



Anonymized Access (0)

Config Compliance (0)

Credential Loss (0)

Data Compliance (0)

File Hosting (0)

Identity Enumeration (0)

Information Loss (0)

Location Anomaly (0)

Open Permissions (0)

Privilege Escalation (0)

Ransomware (0)

Service Disruption (0)

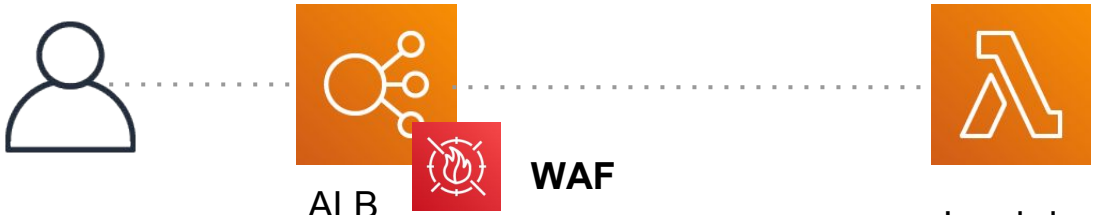
Suspicious Access (0)

WAF - Web Application Firewall

Put a firewall in-front of your **ALB** or **CloudFront**

Two ways to protect Lambdas with WAF

Default Throttled
10K requests per second (rpm)



AWS WAF
Web ACLs
Rules
Marketplace

Conditions
Cross-site scripting
Geo match
IP addresses
Size constraints
SQL injection
String and regex matching

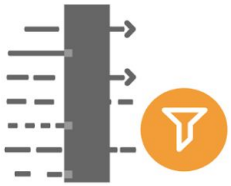
AWS Shield
Summary
Protected resources
Incidents
Global threat environment

AWS FMS
Security Policies
Rule groups

AWS WAF

AWS WAF is a web application firewall service that helps protect the websites and web apps that you deliver with Amazon CloudFront and ELB Application Load Balancers. Create web access control lists (web ACLS) that define which HTTP and HTTPS requests to allow, block, or count. Learn more

Configure web ACL



Web traffic filtering with cus

Create custom rules that can allow, b
count web requests based on origina
addresses or strings that appear in w

ur rules and monitor traffic

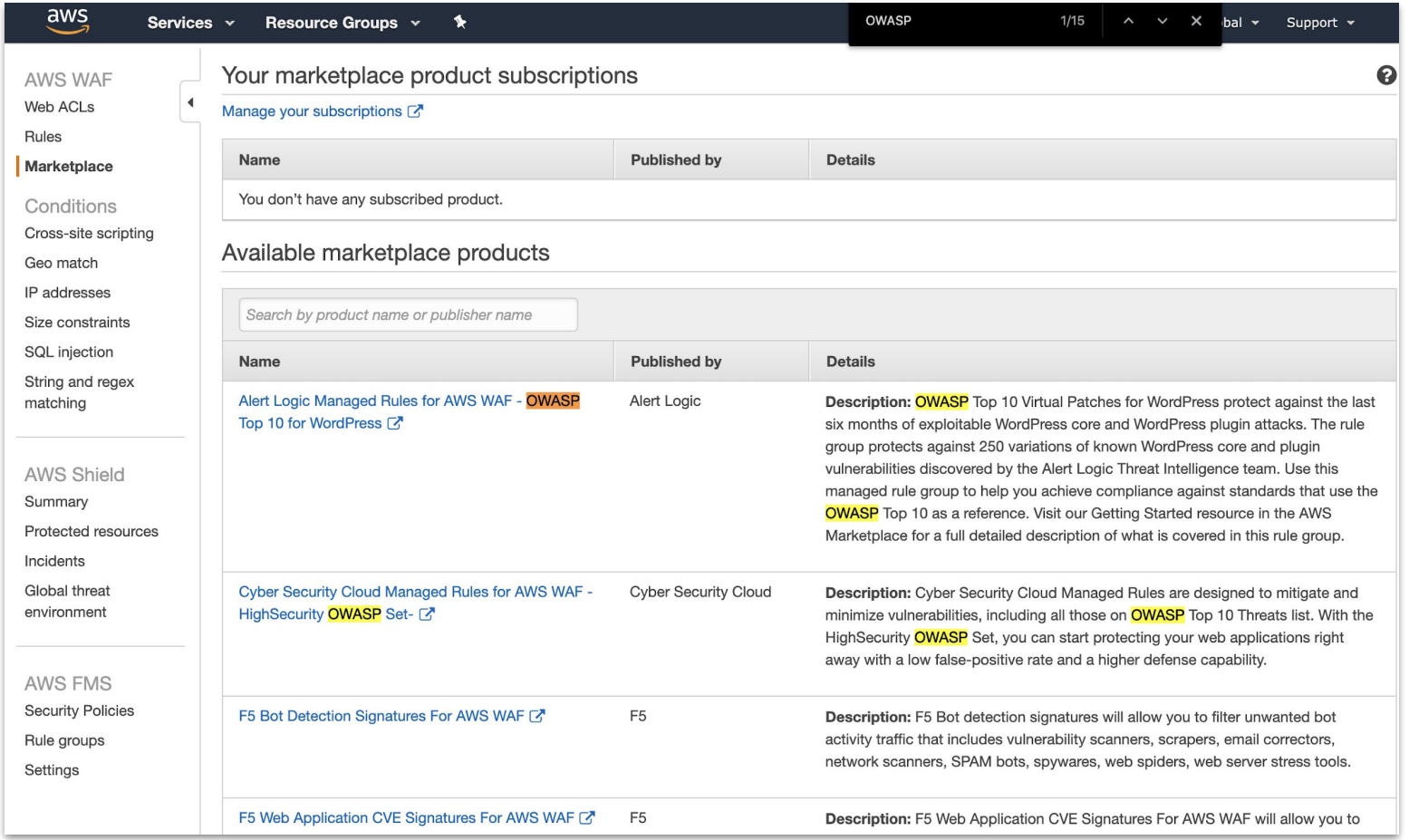
s about the web requests that AWS
blocks, or counts, and update rules
attacks.

$5 per ACL
$1 per Rule

Geo match conditions

Name	Create condition
US	

A geo match condition lets you allow, block, or count web requests based on the geographic origin of the request. Learn more


aws
Services
Resource Groups
OWASP
1/15
bal
Support
AWS WAF
Web ACLs
Rules
Marketplace
Conditions
Cross-site scripting
Geo match
IP addresses
Size constraints
SQL injection
String and regex matching
AWS Shield
Summary
Protected resources
Incidents
Global threat environment
AWS FMS
Security Policies
Rule groups
Settings
Your marketplace product subscriptions
Manage your subscriptions
Name
Published by
Details
You don't have any subscribed product.
Available marketplace products
Search by product name or publisher name
Name
Published by
Details
Alert Logic Managed Rules for AWS WAF - OWASP Top 10 for WordPress
Alert Logic
Description: OWASP Top 10 Virtual Patches for WordPress protect against the last six months of exploitable WordPress core and WordPress plugin attacks. The rule group protects against 250 variations of known WordPress core and plugin vulnerabilities discovered by the Alert Logic Threat Intelligence team. Use this managed rule group to help you achieve compliance against standards that use the OWASP Top 10 as a reference. Visit our Getting Started resource in the AWS Marketplace for a full detailed description of what is covered in this rule group.
Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-
Cyber Security Cloud
Description: Cyber Security Cloud Managed Rules are designed to mitigate and minimize vulnerabilities, including all those on OWASP Top 10 Threats list. With the HighSecurity OWASP Set, you can start protecting your web applications right away with a low false-positive rate and a higher defense capability.
F5 Bot Detection Signatures For AWS WAF
F5
Description: F5 Bot detection signatures will allow you to filter unwanted bot activity traffic that includes vulnerability scanners, scrapers, email correctors, network scanners, SPAM bots, spywares, web spiders, web server stress tools.
F5 Web Application CVE Signatures For AWS WAF
F5
Description: F5 Web Application CVE Signatures For AWS WAF will allow you to

WAF - Web Application Firewall

AWS CloudFormation Template

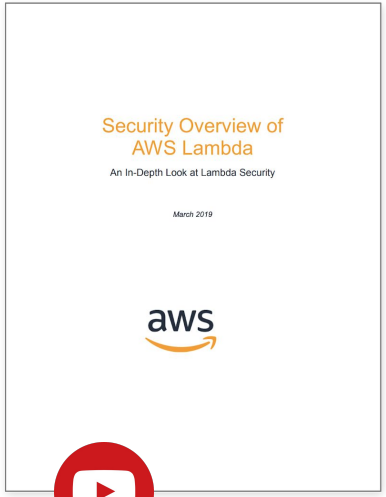
This solution uses AWS CloudFormation to automate the deployment of AWS WAF Security Automations on the AWS Cloud.

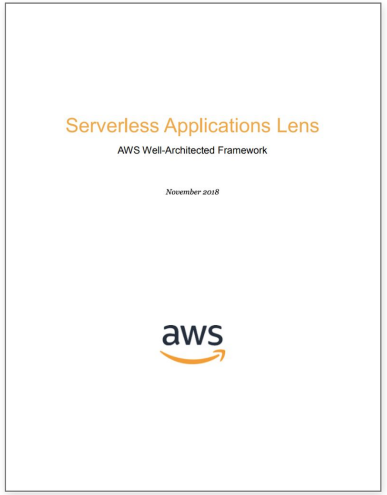
It includes the following AWS CloudFormation template which contains two nested templates: one that deploys AWS CloudFormation and one that deploys an Application Load Balancer.

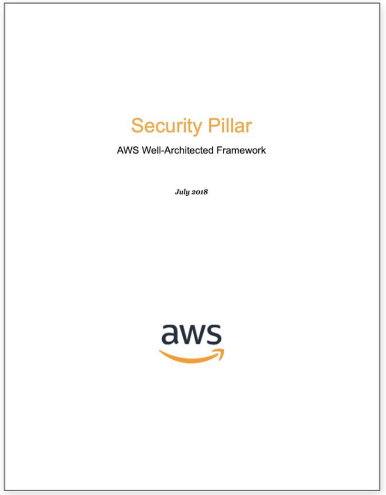
View Template **aws-waf-security-automations.template:** This is the master template used to launch the AWS WAF Security Automations solution for web applications. The default configuration deploys an AWS WAF web ACL with eight preconfigured rules, but you can also customize the template based on your specific needs.

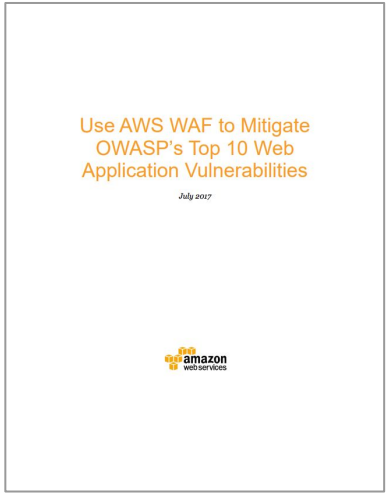
Document Conventions « Previous Next »

Serverless Security AWS Whitepapers





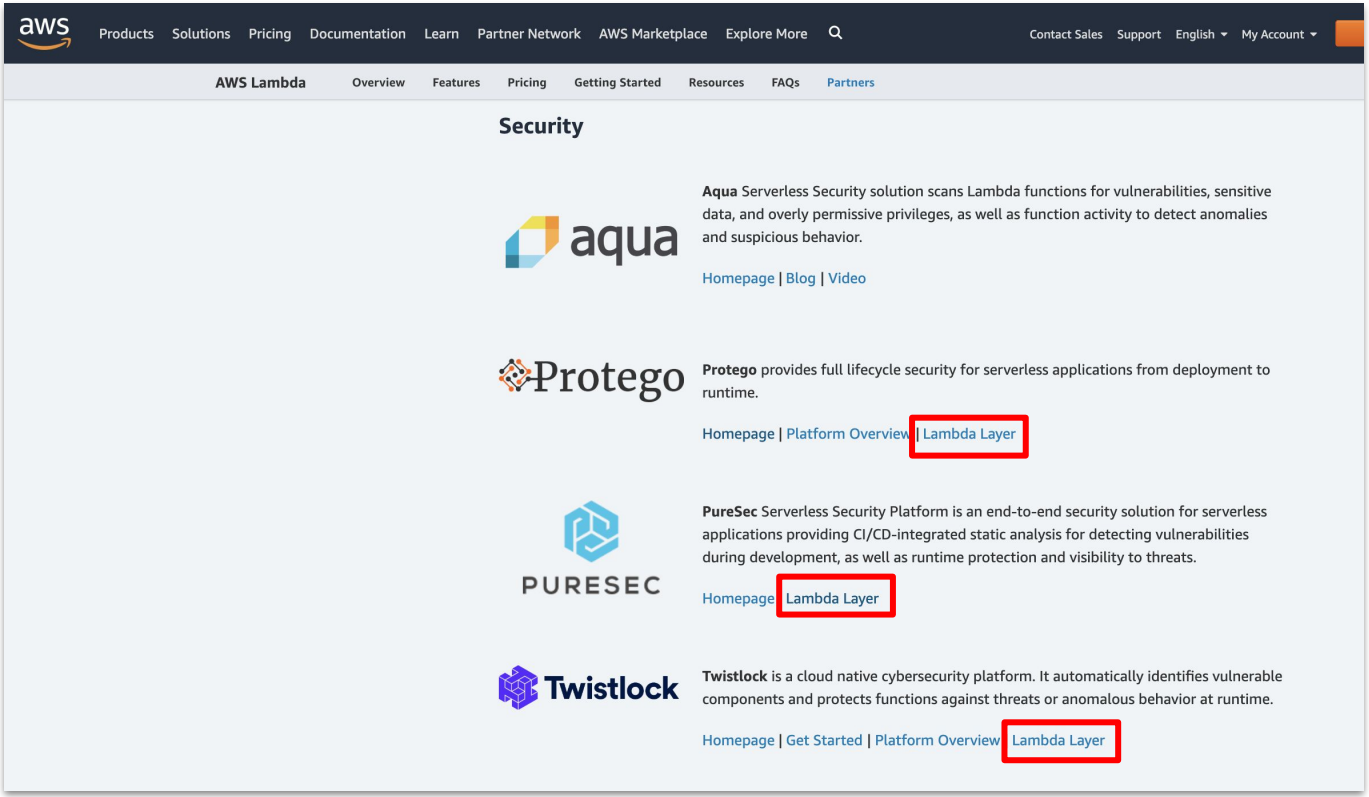




White Paper Video Walkthroughs

https://www.youtube.com/**c/ExamProChannel**

AWS Lambda Security Partners



PURESEC

Serverless Security Platform

AWS Lambda

- ✓ Seamless integration into your CI/CD
- ✓ Checks over-permissive IAM roles
- ✓ Checks insecure storage of app secrets
- ✓ Scans known vulnerable 3rd party dependencies
- ✓ Serverless application firewall
- ★ Behavioural protection engine
- ✓ Security visibility via dashboard and notifications

PURESEC

PRODUCTS RESOURCES BLOG VIDEOS ABOUT GET PURESEC

- ON-DEMAND: FOUNDATIONS OF AWS LAMBDA SECURITY
- ON-DEMAND: SERVERLESS SECURITY 101
- ON DEMAND: JOINT WEBINAR WITH YAN CUI
- ON DEMAND: SERVERLESSDAYS TALK
- WATCH A DEMO

Lambda Security

Ory Segal, CTO and co-founder at PureSec & Jeremy Daly, Serverless Advocate

Exam Pro

Questions? 🤔

Serverless, Startups & AWS

The beginning of a beautiful friendship

Mike Apted – Startup Solutions Architect
@mikeapted
AWS Canada

Enabling Lean Startups with AWS Cloud

Zero upfront cost

With AWS's infrastructure-on-demand, startups can pay only for the resources they use instead of investing in servers upfront

Launch faster

Startups can have new IT resources available in just a few clicks, increasing agility

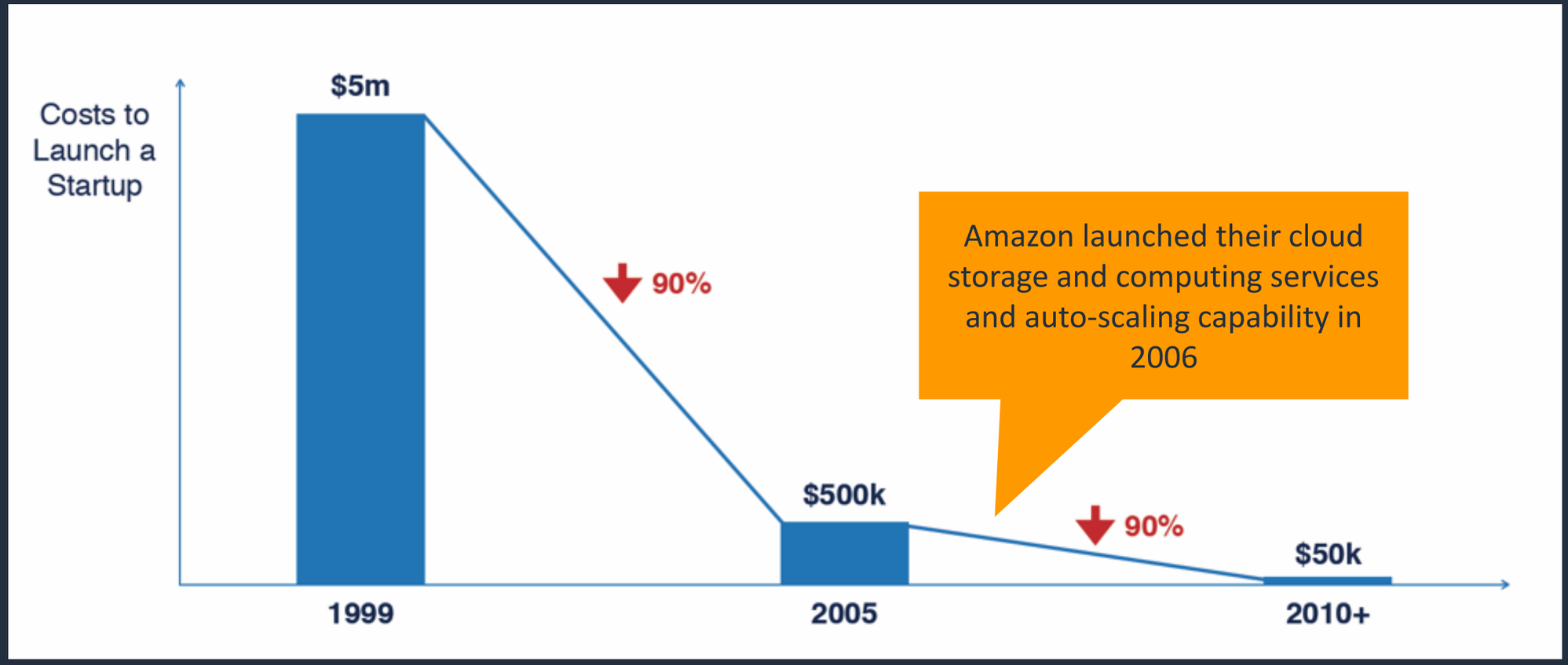
Focus on core business value

Startups can focus on growing their business rather than on infrastructure

Experiment often at lower risk

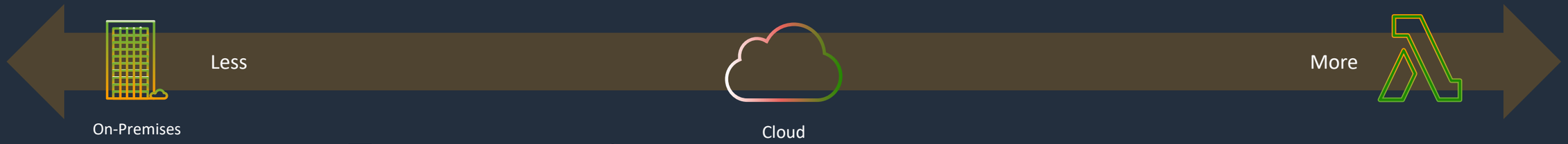
Being able to deprovision resources as needed enables startups to experiment often and fail fast if an idea doesn't work

Massive technology shifts such as cloud computing made it significantly cheaper to launch a startup:



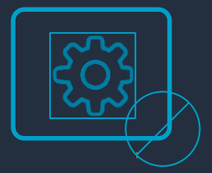
Source: https://bothsidesofthetable.com/why-has-seed-investing-declined-and-what-does-this-mean-for-the-future-6a9572357130

Operational responsibility models



Compute	Virtual Machine	EC2	Elastic Beanstalk		Fargate	Lambda
Databases	MySQL	MySQL on EC2	RDS MySQL	RDS Aurora	Aurora Serverless	DynamoDB
Storage	Storage					S3
Messaging	ESBs		Amazon MQ	Kinesis		SQS / SNS
Analytics	Hadoop	Hadoop on EC2	EMR	Elasticsearch Service		Athena

Startups benefit from serverless:



No infrastructure provisioning, no management

Automatic scaling

Pay for value

Highly available and secure

Serverless is an operational model that spans many different categories of services

COMPUTE

AWS
Lambda

AWS
Fargate

DATA STORES

Amazon
S3

Amazon Aurora
Serverless

Amazon
DynamoDB

INTEGRATION

Amazon
API Gateway

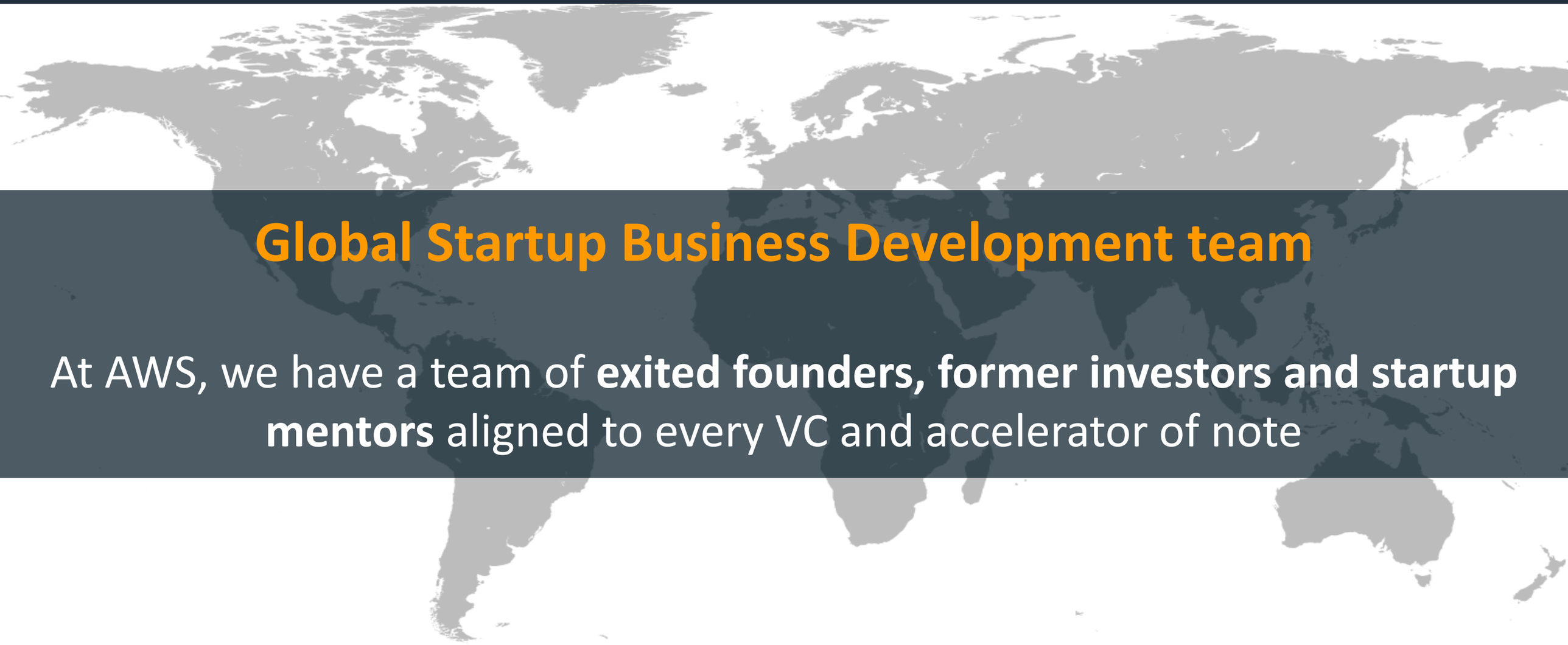
Amazon
SQS

Amazon
SNS

AWS
Step Functions

AWS
AppSync

Beyond technology



Global Startup Business Development team

At AWS, we have a team of **exited founders, former investors and startup mentors** aligned to every VC and accelerator of note

AWS Startup BD/SA: Working with venture capital and the startup ecosystem

Innovation hubs are designed to help, collectively

Maturity of Venture

Type of Hub	Stage	Funding Round	~ Revenue	Timing	Support Provided
Growth Hub	> Self- Sufficient	> A/B	> $5 million	As Needed	•Connections to Customers, Capital and Talent
Scaleup Hub	PMF to Self-Sufficient	Seed → A/B	$1 million →$5 million	As needed	•Peers •Network •Services •Network •Office Space
Accelerator	MVP to Product Market Fit	Angel → Seed	$0 → $1 million ARR	Cohort (3-6 mo)	•Mentors •Network •Programs •Peers •Office Space •Investment
Incubator	0 to MVP	0 → Angel	$0	As needed	•Mentors/Coaches •Guidance •Network •Service Providers

aws

EARLY

STARTUP

SCALEUP

Innovation Hubs

Biomedical Zone
Centre for Business and Student Enterprise
Centre of Urban Energy
Community Innovation Lab
Design Fabrication Zone
DMZ Sandbox
Founder Institute
FoundersBeta
Health Innovation Hub
Humber Centre for Entrepreneurship
Impact Centre
Obio
Spark Centre
Start@UTMAS
The Big Push
The Hub
The Imagination Catalyst
Thunder Road Capital
Zone Startups Sports + Media
The DMZ
Communitech Corporation
Department of Computer Science Innovation Lab
Extreme Accelerator Inc.
Haltech
Hatchery
Highline BETA Inc.
HIGH-LINE.vc
iBoost Zone
ICUBE
IDEABOOST
Innovate Niagara
Innovation Factory
Innovation Guelph
Innovation York
JLABS
Launch180 Accelerator
Legal Innovation Zone
Next Canada
Science Discovery Zone
Social Ventures Zone
The Forge
UTEST
Velocity
ventureLAB
Wilfrid Laurier LaunchPad
York Angel Investors Inc.
MaRS Discovery District

Toronto Business Development Centre (TBDC) Business Incubation
Accelerator Centre
Centre for Commercialization of Regenerative Medicine
Food Starter
GreenCentre Canada
LatAm Hub Toronto
Ontario Agri-Food Technologies
RIC Centre
Seneca HELIX
Tech Alliance
Ontario Centres of Excellence
MaRS Discovery District

oneeleven
The Lazaridis Institute for the Management of Technology Enterprises
Bioentreprise Corporation
Tech Place
MaRS Discovery District

TORONTO-WATERLOO CORRIDOR

Startup Ecosystem

STAGES

- Early
- Startup
- Scaleup
- Growth

BUSINESS TYPES

- Angel Group
- Development
- Financial Advisory
- Incorporated
- Accelerator
  - Campus Linked
  - Corporate
  - Government Backed
  - Private / Non-Profit
- Law Firm
- Management Consultants
- Marketing
- Private Equity
- Venture Capital

Powered by Hockeystick

hockeystick.co @hockeystick

We invest *indirectly* alongside venture funds and accelerators

We don’t

- Invest cash
- Take a capital position

We do

- Invest time
- Share knowledge/experience/wisdom
- Help navigate AWS resources and support
- Open doors internally and externally
- Remove obstacles
- Leverage our global footprint
- Champion startups across all of Amazon
- Take a long-term view

We focus on helping our startup customers grow

by wiring them into people, resources, opportunities across Amazon

Technical

- Architecture design/optimization reviews
- Best practices
- Subject matter experts
- Betas/previews
- Security/compliance

Go-to-market

- Co-marketing
- PoC funding
- Sales referrals
- Distribution
- Capital intros

Amazon programs that help startups grow their business

**Eligibilities and limits apply*

AWS Activate

- AWS promotional credits
- AWS Business Support Plan
- Online training credits
- Office hours

AWS Migrate

- Credits that help offset cost of migration (limited time)
- Technical migration support

AWS Well-Architected Review

- Free review by AWS Solution Architects
- Ensures secure, high-performing, resilient, efficient infrastructure

AWS Connections

- Introduction to enterprises with a specified solution need

AWS Partner Network

- Tiered funding benefits
- Technical training
- Sales and business enablement
- Co-marketing

AWS Marketplace

- Streamlined go-to-market on AWS's software marketplace
- Integrated billing with AWS

Amazon Launchpad

- Dedicated launch and marketing support for selling physical product on amazon.com

Alexa Fund

- Equity investment for voice technology startups
- Development and marketing support and benefits

…and more! Contact your AWS Startup Business Development Manager for details.

Assistance to grow

Alexa Fund

Benefits

- Equity investment
- Early access to SDK capabilities
- Hands-on development support
- Marketing support
- Placement at Amazon showcase events

Eligibility

- Product benefits from the Alexa Voice Service or delivers new abilities to Alexa-enabled devices through the Alexa Skills Kit
- Contributes to the science behind voice technology

More information

- Alexa Fund website

Assistance to grow

Benefits

- Mentorship and network from across Amazon and Techstars networks

Eligibility

- Product benefits from the Alexa Voice Service or delivers new abilities to Alexa-enabled devices through the Alexa Skills Kit
- Contributes to the science behind voice technology

More information

- Amazon Alexa Accelerator website

aws

Startup Migrate Program

Removing barriers to adoption

Benefits

- Credits that help offset cost of migration (limited time)
- Technical support (partner funding, AWS Support Plan)

Eligibility

- Speak with an AWS startup BD manager for details

More information

- Featured startup migrations on AWS Startup Blog

Support at the earliest stages

aws activate

Benefits

- AWS promotional credits
- Business Support Plan
- Online self-paced lab credits
- Office hours
- Startup Spotlight

Eligibility

- Startups in accelerators, incubators, early VC funds or other startup organizations (ex. university programs, co-working spaces, etc.)

More information

- AWS Activate website

aws

doorr

THE DOORR PLATFORM

SOLVED MULTIPLE PAIN POINTS

USING SERVERLESS ARCHITECTURE

TOP OBSTACLES

PROVISIONING SERVERS

PAYING FOR SERVER IDLE TIME

SCALING FOR USAGE

RESULTS

$280

NET MONTHLY COST

3 MONTHS

TIME TO BUILD CORE PLATFORM

24 MILLION

TRANSACTIONS PER MONTH

WITHOUT SERVERLESS

DOOR'S GROWTH WOULDN'T BE SUSTAINABLE

DUE TO INFRASTRUCTURE COSTS.

Thank you!

Mike Apted – Startup Solutions Architect
@mikeapted
AWS Canada