

# “Can We See Everything That We Need To In The Cloud? – That’s A Question We Just Can’t Answer Yet”

---

Private University

**“Our SaaS Providers Handle The Security Of The Cloud Service But We Are Worried About Cloud Being Used As An Attack Vector”**

---

Large State School

# “Hahahahaahahaha”

---

- Customer when asked how the cloud shift was going

splunk®

.conf2017

© 2017 SPLUNK INC.

# Using ES to Secure the Cloud

Relief from the headache in the cloud

David Naylor | Security Analyst, Georgetown University

Craig Vincent | Regional Security SME, Splunk

Date | Washington, DC



# Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.









# Challenges of Moving to the Cloud

---

# Challenges of Moving to the Cloud

Lack of Visibility



**61% of survey  
respondents say its  
difficult to get  
equivalent visibility  
into cloud-based  
workloads**

Enterprise Strategy Group 2017









# Introduction to Enterprise Security

---

# Introduction to Enterprise Security

## Advanced Threats are Hard to Find




**Cyber Criminals**




**Nation States**




**Insider Threats**




**100%**  
Valid credentials were used



**40**  
Average # of systems accessed



**229**  
Median # of days before detection



**67%**  
Of victims were notified by external entity

Source: Mandiant M-Trends Report 2012/2013/2014

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product\_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"  
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D15L9FF1ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product\_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"  
125.17.14 - - [07/Jan 18:10:55:187] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"  
125.17.14 - - [07/Jan 18:10:55:189] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"





# Introduction to Enterprise Security

## Why Enterprise Security

- ▶ Native to the Cloud
- ▶ Integrates on premise Security with Cloud Security
  - Single Pane of Glass
  - Single Workflow
- ▶ Flexibility
  - Able to ask any question
  - Change friendly

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&SESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=F1-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=K0-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"  
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&SESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"  
10.0.0.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category\_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"

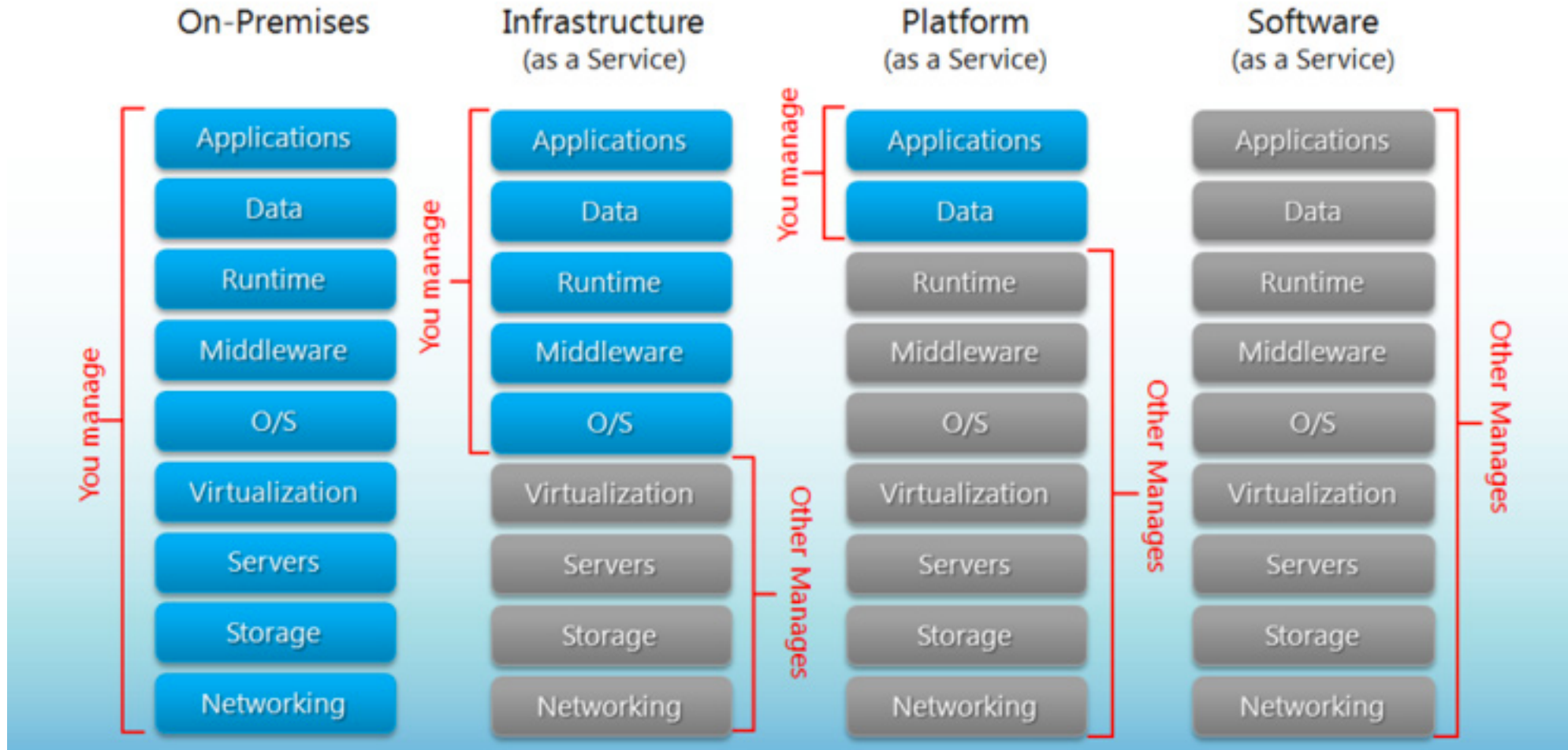




# Uncovering the Cloud

---

# Comparison of Cloud Services





# Comparison of Cloud Services

## Security Responsibility

### SaaS

#### Software as a Service

- Access and Authentication
- Data Transit to the Cloud
- Misuse

- Other security responsibilities tend to lie with the vendor

### PaaS

#### Platform as a Service

- Application Security
- Auditing

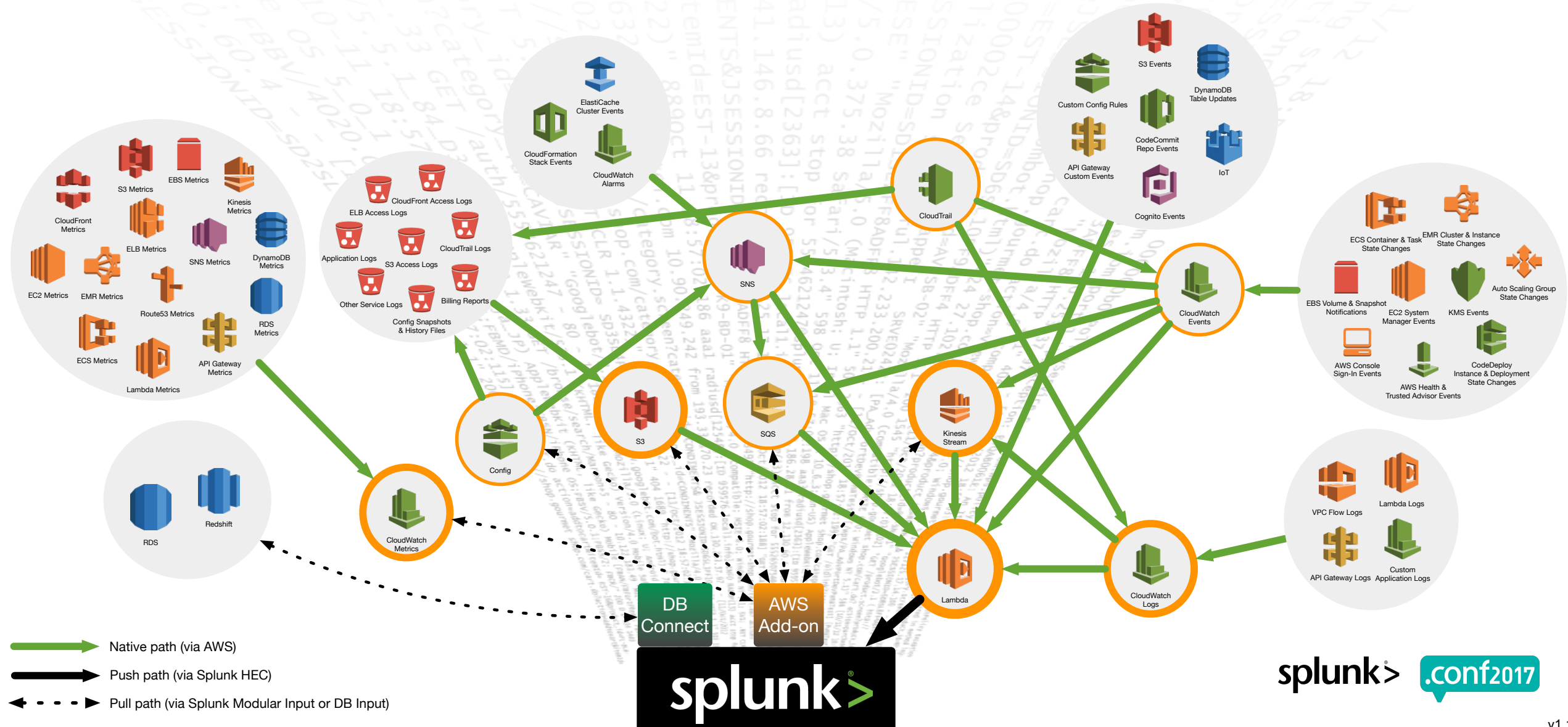
- Networking Configuration

### IaaS

#### Infrastructure as a Service

- Responsible for all security except for infrastructure security

# End-to-End Visibility with AWS and Splunk





# Georgetown ES

---







# Georgetown & ES

## Policy Enforcement Correlation Search

- ▶ AWS security groups are the firewall policy for the EC2 instance
- ▶ At Georgetown, we flag all instances that are set to allow all to push users towards specific firewall rules

Policy Enforcement Correlation Search  
[Go to Content Management](#)

### Correlation Search

Search Name \*

Application Context \*

UI Dispatch Context \*

Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.

Description

Describes what kind of issues this search is intended to detect.

# Georgetown & ES

## Cloud Data Enrichment

- ▶ Gather cloud context by updating ES asset table using AWS Description logs

The screenshot shows the Splunk search interface with a search query and a table of results. The query is as follows:

```
(index="main" sourcetype="aws:description" aws_account_id="*" region="*" source="*:ec2_instances")
| eventstats latest(_time) as latest_time
| eval latest_time=relative_time(latest_time,"-55m")
| where ('_time' > latest_time)
| dedup id sortby -_time
| dedup private_ip_address
| eval ip=if(ip_address!="null",private_ip_address."|".ip_address,private_ip_address)
| eval dns=if(dns_name!="",private_dns_name."|".dns_name,private_dns_name)
| rename "tags.App Manager" as tagsappmanager
| eval owner=if(isnull(tagsappmanager),"",tagsappmanager)
| eval priority="medium"
| eval platform=if(platform=="null","",|.platform)
| eval category=placement."|".instance_type."|".state.platform
| rename vm_name as nt_host
| table ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should_timesync,should_update,requires_av
```

The search results show 44 events from 8/18/17 5:00:00.000 PM to 8/19/17 5:07:05.000 PM. The table below shows the first few columns of the results:

ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category

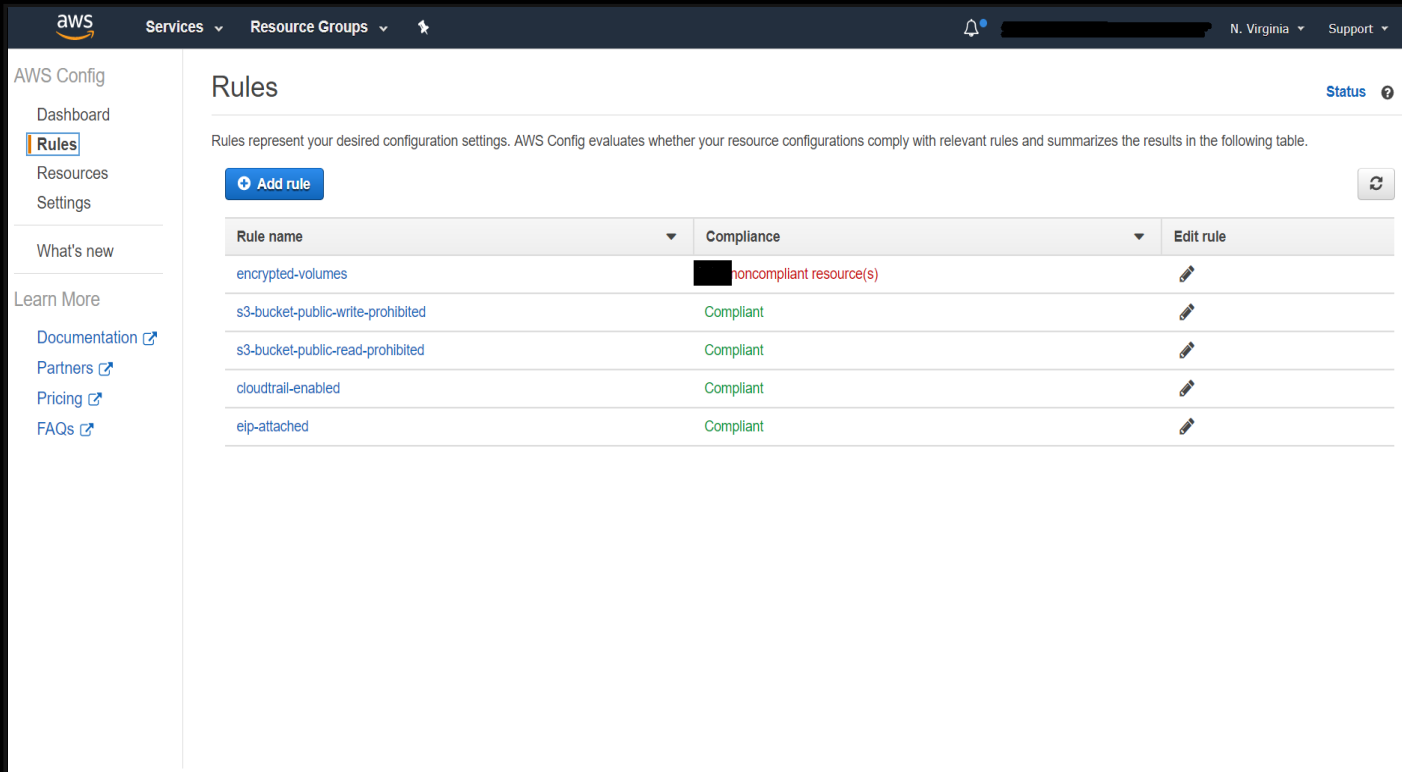






# Georgetown & ES

## Using Lambda to find bad configurations



The screenshot shows the AWS Config console interface. The left sidebar contains navigation options: Dashboard, Rules (selected), Resources, Settings, What's new, and Learn More (Documentation, Partners, Pricing, FAQs). The main content area is titled 'Rules' and includes a description: 'Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.' Below this is an 'Add rule' button and a table of rules.

Rule name	Compliance	Edit rule
encrypted-volumes	noncompliant resource(s)	
s3-bucket-public-write-prohibited	Compliant	
s3-bucket-public-read-prohibited	Compliant	
cloudtrail-enabled	Compliant	
eip-attached	Compliant	

At the bottom of the console, there is a footer with 'Feedback', 'English (US)', and copyright information: '© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Us'.

- ▶ AWS config rules use a lambda instance to affordably ensure configuration compliance



# Takeaways

1. Understand your level of responsibility
2. IaaS providers provide rich logging for increased visibility
3. ES helps with the entire IR lifecycle

# CLOSING REMARKS & CALL TO ACTION

---

# splunk> .conf2017

Public Sector & Education Industry Day at .conf2017  
Wednesday, September 27<sup>th</sup>, 2017  
11:00am-7:00pm | Room 202A



**400+**

Attendees



**5**

Sessions



**15**

Customer  
Speakers



**10+**

Birds of  
Feather  
Sessions



splunk® **.conf2017**

# Public Sector Birds of a Feather

Meal Room (Lower Level Hall B)

Wednesday, September 27<sup>th</sup>

1:15pm-2:00pm

Compliance  
Security  
IT Modernization  
Situational Awareness  
Mission Analytics

Institutional Intelligence  
Learning Analytics  
Supply Chain  
Smart Communities  
Cloud

splunk®

.conf2017

© 2017 SPLUNK INC.

# Public Sector Reception

Walter E. Washington Convention Center  
South Pre-Function Space on Level 3

5:30pm-7:00pm

Join Splunk and your peers for hors d'oeuvres and drinks.  
Unwind, discuss hot topics and share your stories!

*\*.conf badge required for entry*

# Thank You

Don't forget to **rate this session** in the  
.conf2017 mobile app

splunk® **.conf2017**