



Splunk on AWS

Igor Alekseev
Partner Solution Architect | AWS

splunk>

.conf19

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. © 2019 Splunk Inc. All rights reserved.

“Our partnership with Splunk is incredibly important for our customers. Customers love **AWS agility with **Splunk visibility**.”**

- ▶ Andy Jassy, CEO, Amazon Web Services

Splunk's AWS Credentials

- ❑ AWS Advanced Technology Partner
- ❑ AWS Big Data Competency
- ❑ AWS Security Competency
- ❑ AWS DevOps Competency
- ❑ AWS Government Competency
- ❑ AWS Education Competency
- ❑ AWS IoT Competency
- ❑ AWS MSP Technology Provider
- ❑ AWS Marketplace Partner
- ❑ AWS Security by Design Program Partner



Why is Splunk Important for AWS Customers?

**“You can’t
protect what
you can’t
see.”**

**Best Practices for Securing
Workloads in Amazon Web
Services**

*Gartner, Neil MacDonald, Greg
Young*

**“Security
monitoring will
make or break a
technology risk
management
program.”**

**Assessing the Risk: Yes, the
Cloud Can Be More Secure Than
Your On-Premises Environment**

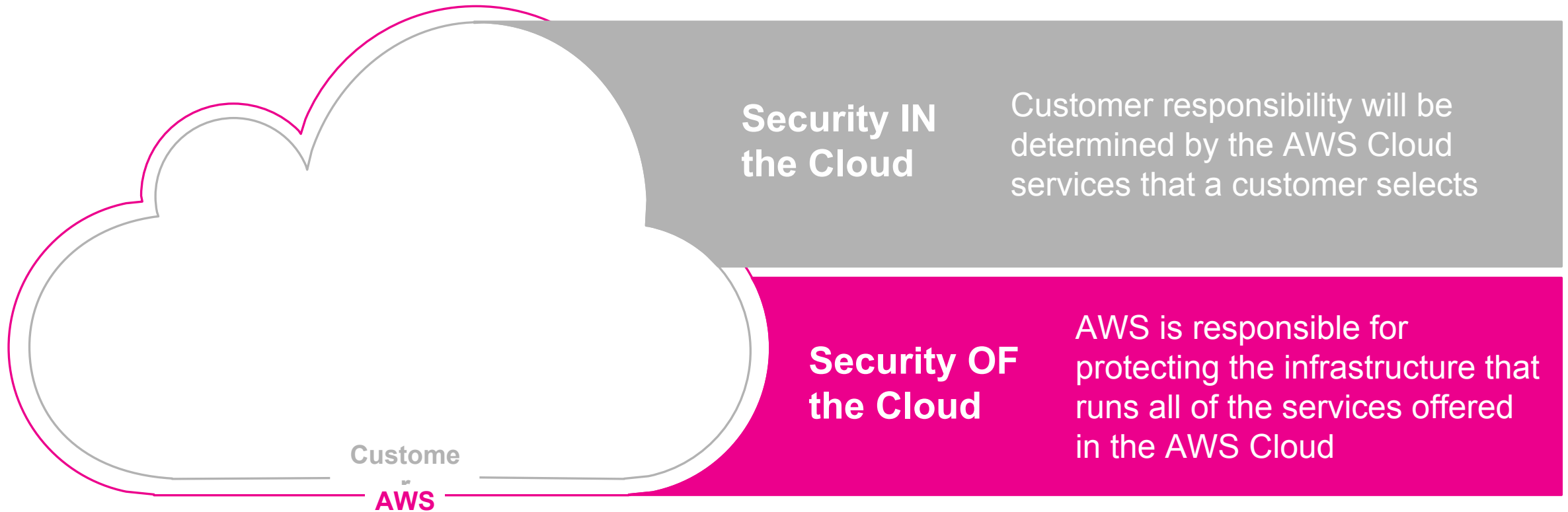
IDC, Pete Lindstrom

**“Security
requires
visibility.”**

**Amazon Web Services
“Intro to AWS Security”**

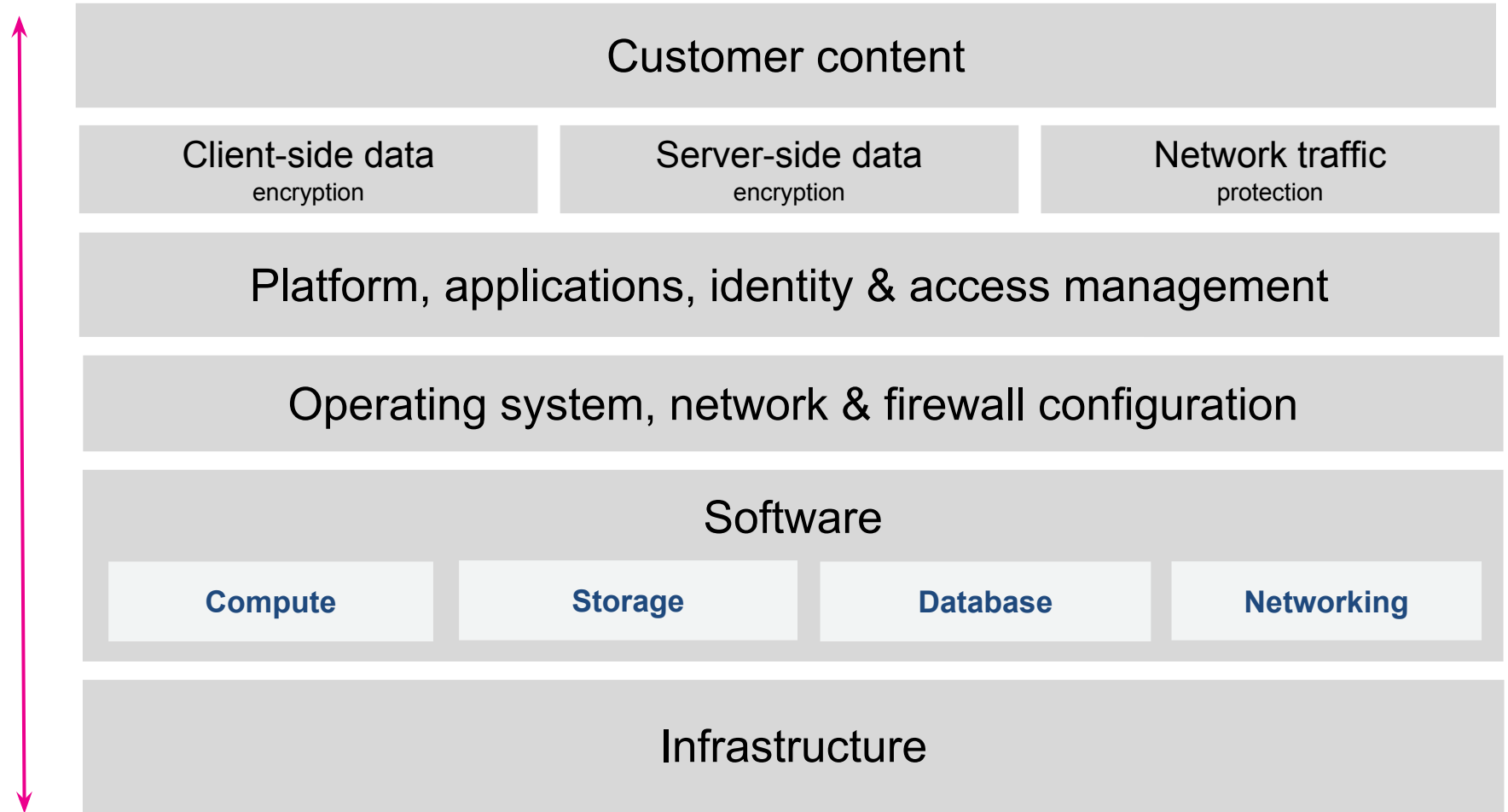
AWS Summit Series

Shared responsibility model



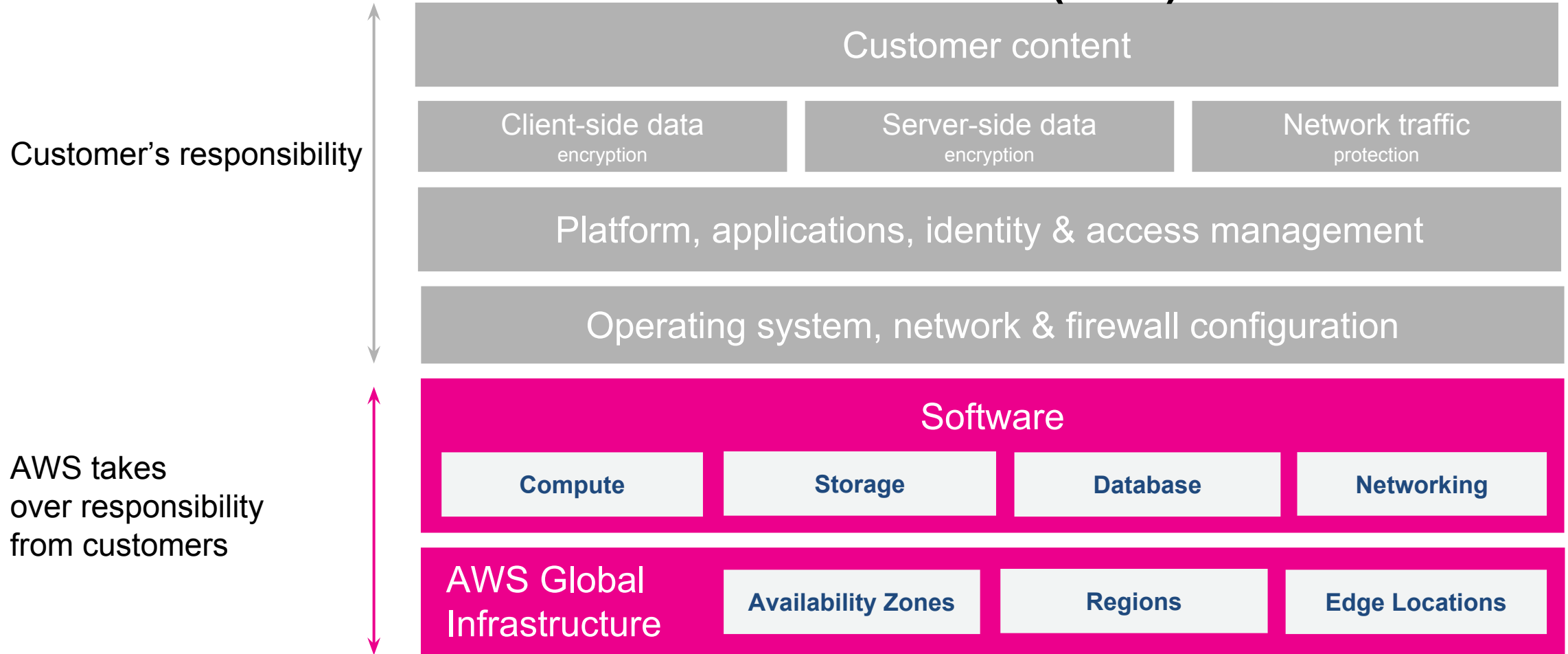
Traditional on-premises security model

Customers are responsible for end-to-end security in their on-premises data centers



AWS / Customer shared responsibility

Infrastructure as a Service (IaaS)



Splunk's Approach to Cloud Monitoring



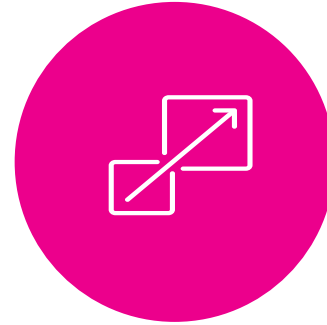
Cloud Migration

Get visibility at all stages of the migration process – whether before, during or long after.



Manage Hybrid Infrastructure

Hybrid infrastructure creates a complex monitoring environment. Legacy tools can't keep up. Splunk can.



One Consolidated Solution

Splunk takes the place of the multitude of monitoring tools because sometimes one is better than many.



Cost, Capacity, and Resource Management

Understand how your resources are performing – and how many are being used – then optimize utilization and billing

Migrate securely to AWS with Splunk

An REI case study



Company overview

REI is a national outdoor retail co-op dedicated to inspiring, educating, and outfitting its members and the community for a lifetime of outdoor adventure and stewardship.

\$2.6B

2016 Revenue

17M

Co-op members

154

Retail stores in
36 states

Challenges

REI needed to extend its security posture to include edge protection of its Amazon Virtual Private Clouds (VPCs) as it migrated application to AWS.

It was determined that REI previously lacked:

- A solid investigation workflow that included its AWS deployment
- A secure ingress path for migrating applications to AWS
- A clear path for implementing a DevSecOps practice across all REI accounts and VPCs

Splunk is available in AWS Marketplace

Options for Splunk Cloud & Splunk Enterprise

AWS Marketplace Ease of Sale

- Easily discover & deploy software & SaaS
- **Simplified buying process** and consolidated AWS Billing reduces time to procure
- **Automatic renewals**
- One consolidated AWS bill
- Potential impact and “draw-down” on AWS **EDP (Enterprise Discount Program) Contracts**



[Explore AWS Marketplace](#)

Splunk Specifics

- Annual contract subscriptions & automatic discount for multi-annual options
- Buy Splunk Cloud in **increments of 5GB to 100GB** across all supported regions
- Easily upgrade Splunk license
- **Marketplace seller private offers** available for larger index volumes, apps and add-ons
- **Splunk Enterprise licensing** available via AWS Marketplace seller **private offers**

New! [Splunk Insights for Infrastructure Pay-as-You-Go](#)

The AWS & Splunk solution

AWS Services Used:

- Amazon Virtual Private Cloud
- AWS Application Load Balancer (ALB)
- Amazon GuardDuty
- AWS Config
- Amazon CloudWatch

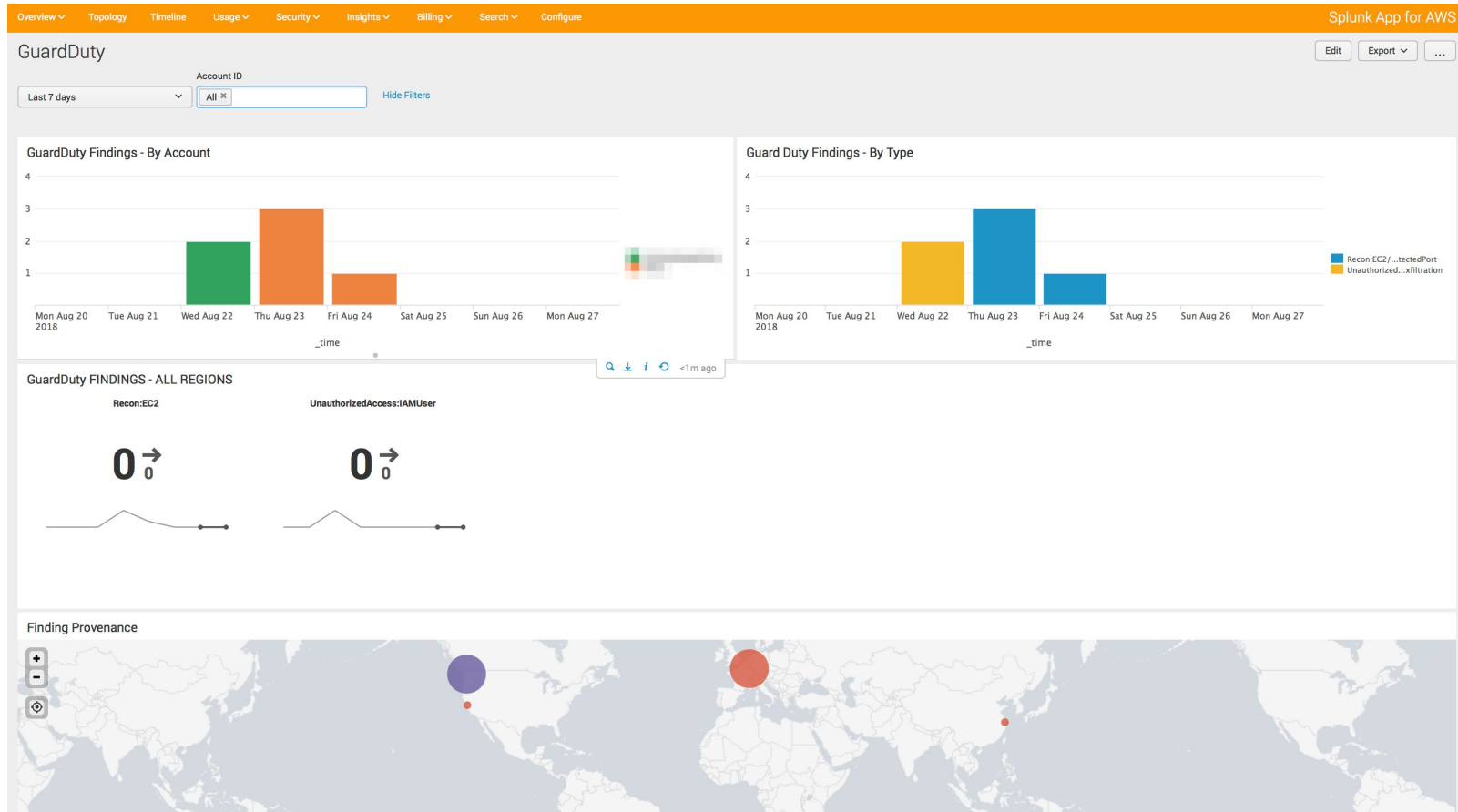
Splunk Products Used:

- Splunk Cloud
- Splunk Enterprise Security
- Amazon GuardDuty Add-on for Splunk
- Splunk App for AWS
- Splunk Add-on for Amazon Web Services

“The largest gain was through securing at the edge. This removed the need for individual dev teams to come up with edge protection models for public-facing endpoints. Splunk is helping us aggregate the Amazon VPC flow logs, AWS Application Load Balancer logs and Amazon GuardDuty logs for easy correlation, visualization and alerting.”

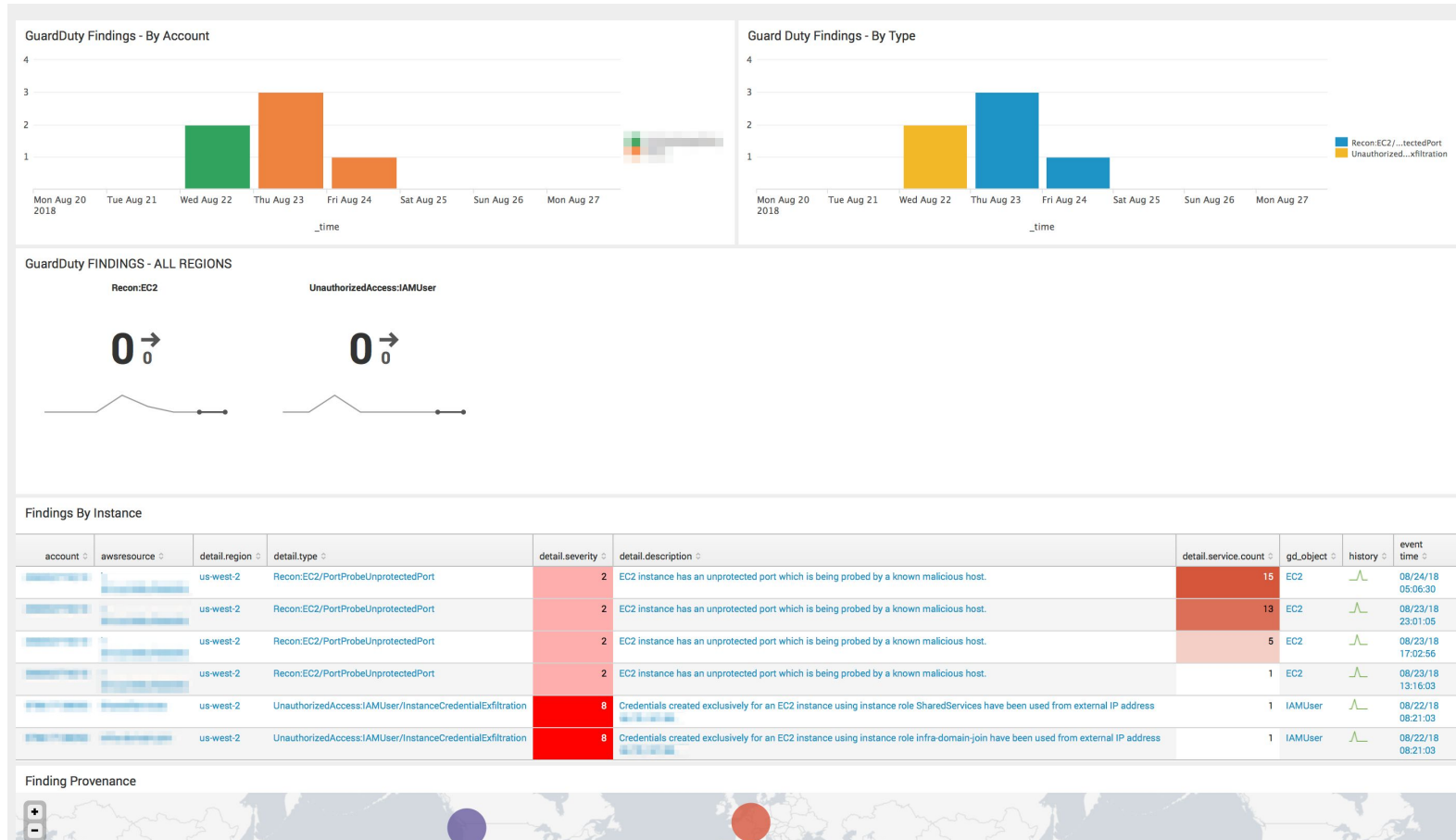
David Bell, Manager, Infrastructure and Cloud Services, REI

Splunk GuardDuty dashboard



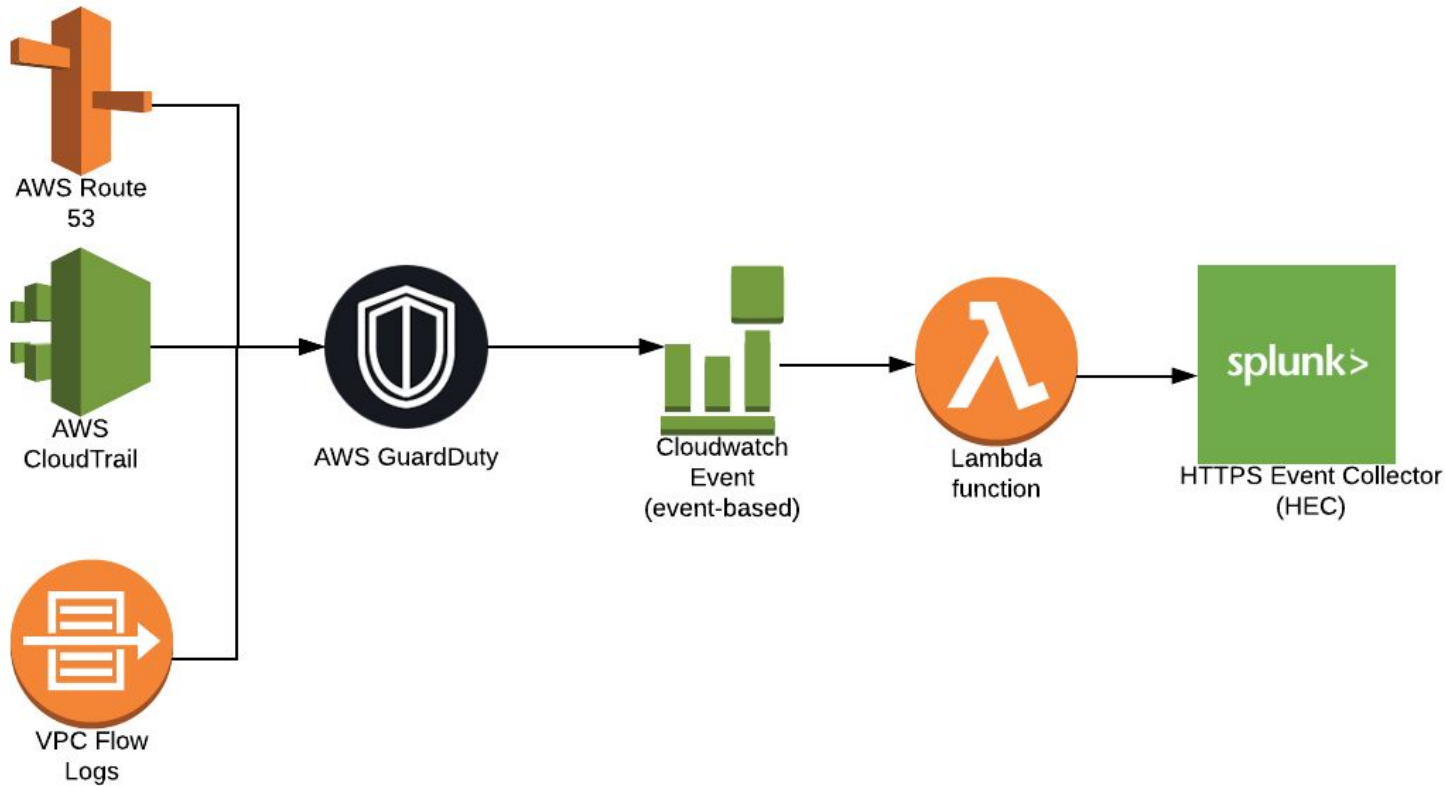
- Moved Amazon GuardDuty findings to Splunk App for AWS to give security engineers a single source of information.
- Created panels to quickly see number of findings per account and overall numbers per finding type.
- Implemented dropdowns for time frame and to select individual AWS accounts.

Splunk GuardDuty dashboard



- Updated hidden drill down panel to work with new custom panels.
- Quickly gives security engineers information concerning AWS accounts, Amazon EC2 instances, and AWS IAM roles.

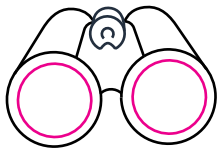
Splunk GuardDuty data flow



- AWS GuardDuty analyzes information from Route 53, CloudTrail, and VPC Flow Logs.
- AWS Cloudwatch Event triggers a Lambda. Immediately for the first alert, every six hours afterwards.
- Lambda function sends CloudWatch data to a Splunk HTTPS Event Collector.
- Note: The Splunk Lambda blueprints and video was extremely helpful in getting this configured.

Business benefits

REI gained:



Real-time visibility
across applications,
services, and security
infrastructure



Threat intelligence,
alerting, security monitoring,
and troubleshooting



Enhanced edge security
as applications migrate to
AWS



Faster time-to-value and
ease of use which reduces
staffing challenges

Splunk and AWS

Index Untapped Data: Any Source, Type, Volume



Ad hoc search



Monitor and alert



Report and analyze



Custom dashboards



Developer Platform

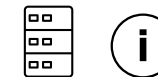
AWS App & Add-on

Real-Time Machine Data

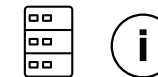
splunk>



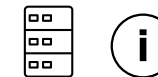
References – Coded fields, mappings, aliases



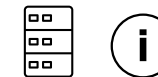
Dynamic information – Stored in non-traditional formats



Environmental context – Human maintained files, documents



System/application – Available only using application request



Intelligence/analytics – Indicators, anomaly, research, white/blacklist

Splunk's approach to AWS migration



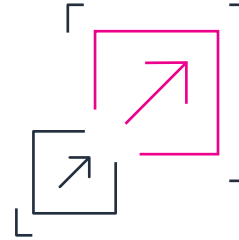
AWS Migration

Get visibility at all stages of the migration process – before, during, and after. Baseline performance and cost metrics.



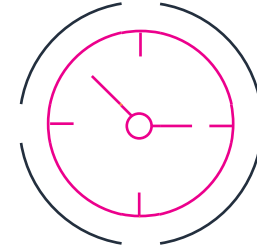
Manage Hybrid Infrastructure

Hybrid infrastructure creates a complex monitoring environment. Splunk enables you to keep up.



One Consolidated Solution

Manage security and IT Ops. Monitor service-level down to system-level in a single view.



Cost, Capacity, and Resource Management

Understand how resources are performing – measure against baselines – then optimize utilization and billing.

Splunk Portfolio of AWS Solutions

End-to-End AWS Visibility

splunk>
App for AWS

Available on Splunk Enterprise, Splunk Cloud and Splunk Light

Integrates with AWS CloudTrail, Config, Config Rules, VPC Flow Logs, Inspector, Billing, CloudFront, ELB Access Logs, S3 Access Logs, Personal Health, & CloudWatch

Self-deployed software on AWS

splunk>enterprise



splunk>



AWS Quick Starts

AWS-based SaaS

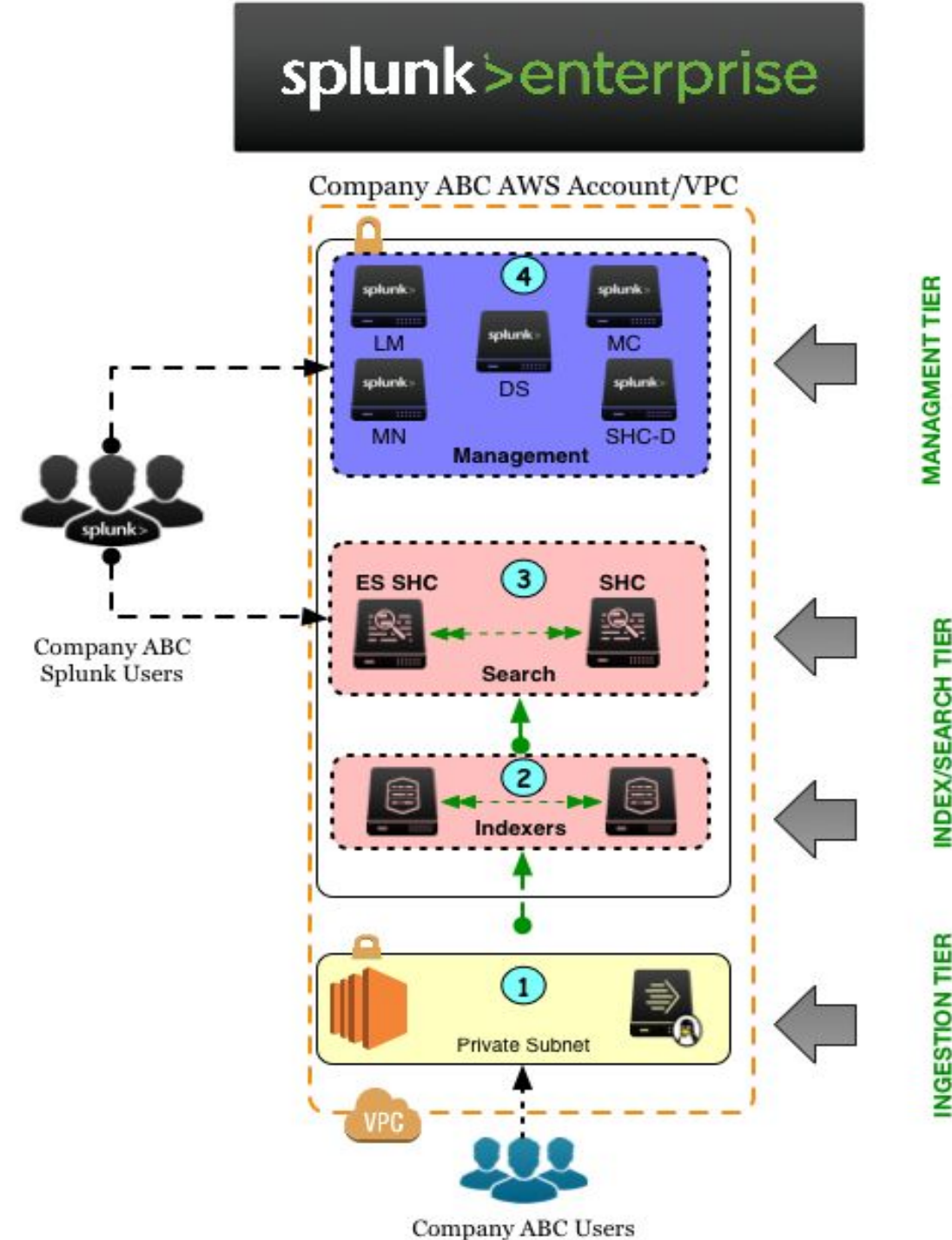
splunk>cloud



Architecture Layers

3 Primary Components

- Ingestion (Data Acquisition)
- Index/Search (Map Reduce/Query)
- Management



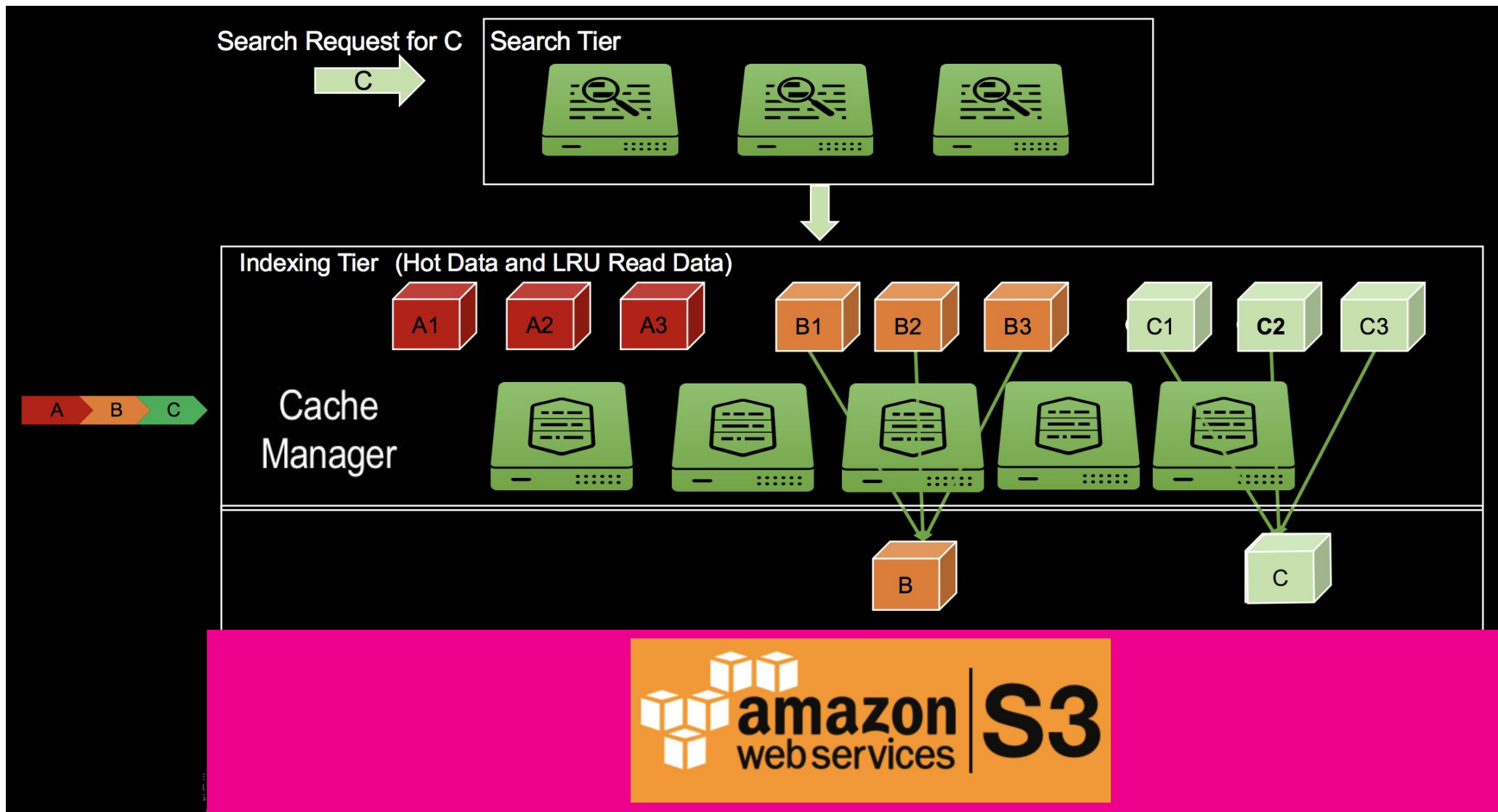
Architecture Tips

Splunk – Indexer Data Replication (IDR)



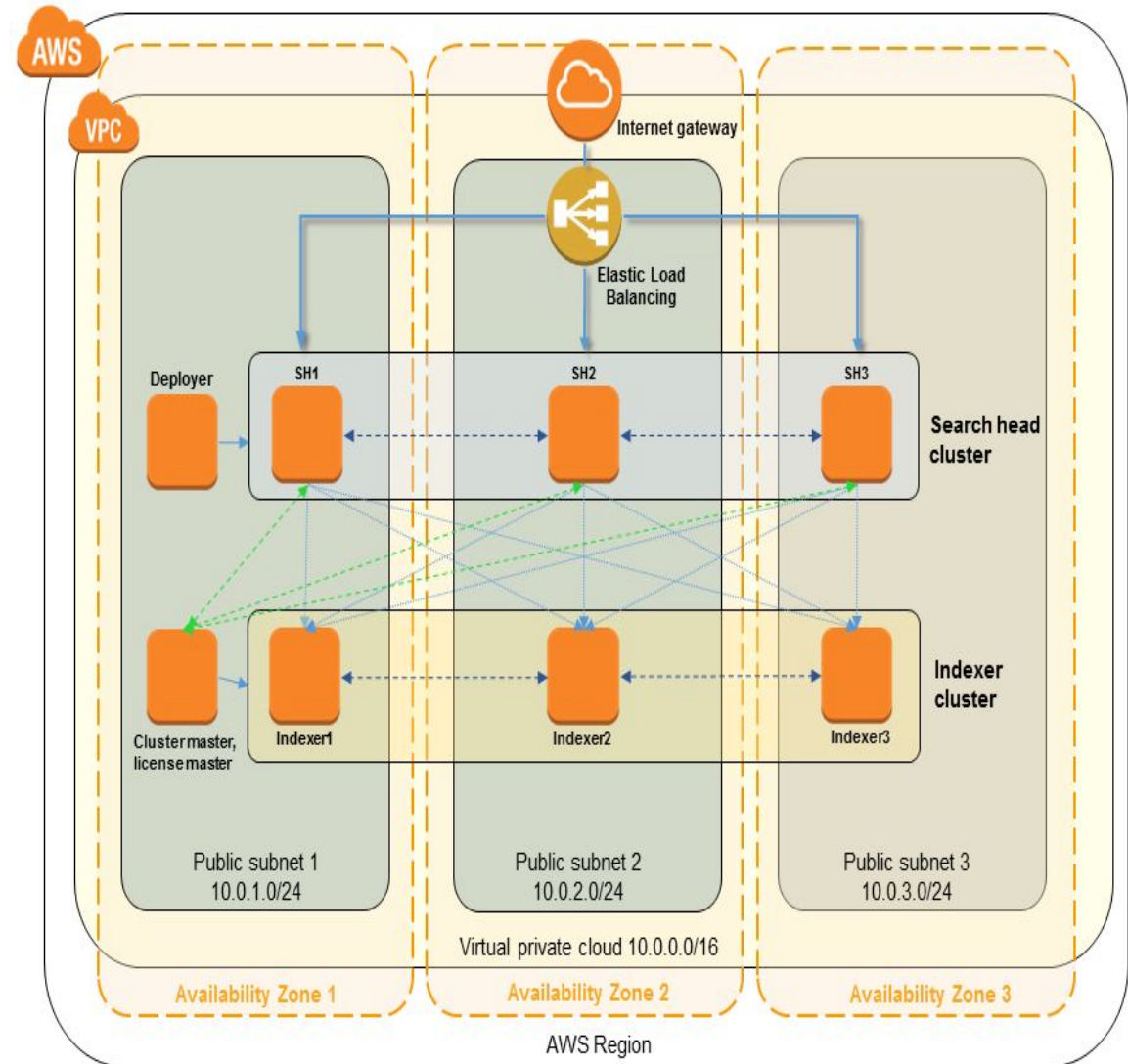
Adding new indexers in response to data growth is expensive □ High cost
Searches typically run over only on a partial subset of data □ Inefficient utilization

Splunk – Smart Store (S2) (Only available for Splunk 7.2 and above)



Splunk AWS QuickStart (IDR only) – Splunk in 45 mins

- Splunk indexer cluster with the number of indexers you specify (3-10)
- Splunk search heads, either stand-alone or in a cluster
- Splunk license server and indexer cluster master
- Splunk search head deployer
- (Optional) User-provided Splunk apps and/or add-ons

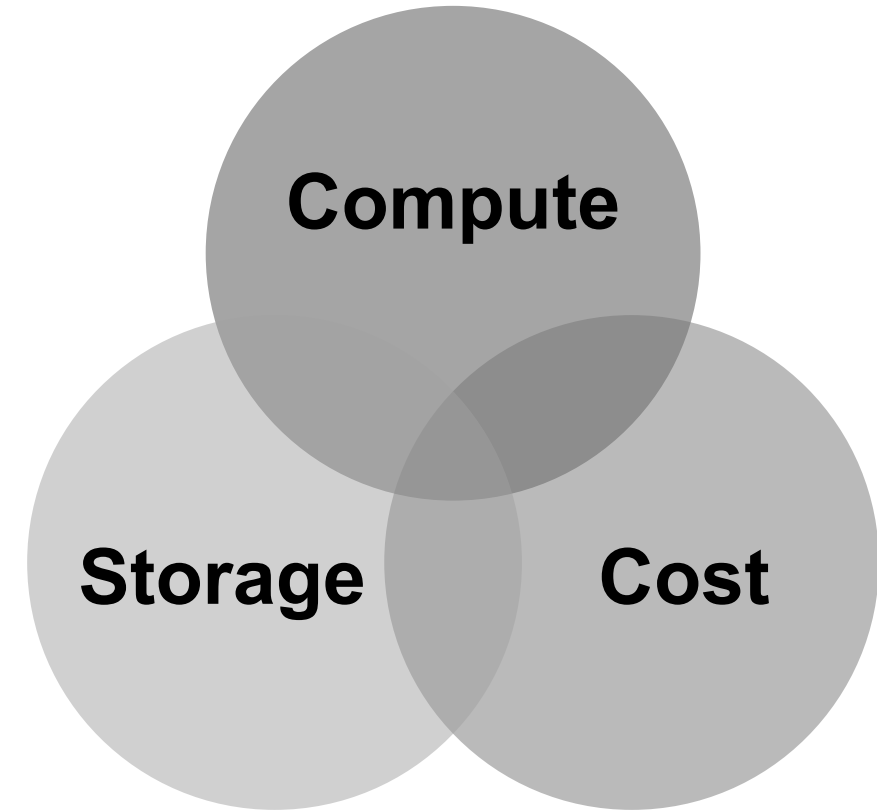


HA & DR Strategy

- ▶ Determine required level of failure tolerance:
- ▶ AZ | Region | Combination thereof

Instance Type Selection Strategy

- ▶ Selecting a base instance type is a **balancing act between compute, storage and cost**.
- ▶ C5, M5 and I3 types are good choices for Indexers and Search Heads.
- ▶ EBS, though redundant in the backend, cannot replace indexer clustering and for some instance types is mandatory
- ▶ SSD ephemeral storage for D and I instance types performs very well but should be used only in clustered deployments



Instance Selection Examples

| Instance Type (Indexer) | Daily Index Volume in GB |
|-------------------------------------|------------------------------|
| c5.9xlarge (IDR) or i3.4xlarge (S2) | Up to 100 |
| c5.9xlarge (IDR) or i3.8xlarge (S2) | Up to 300/250 – 1TB -> 4 IDX |

| Instance Type (Search Head) | Concurrent Users |
|-----------------------------|------------------|
| c5.9xlarge – Core, ES | Up to 16 |

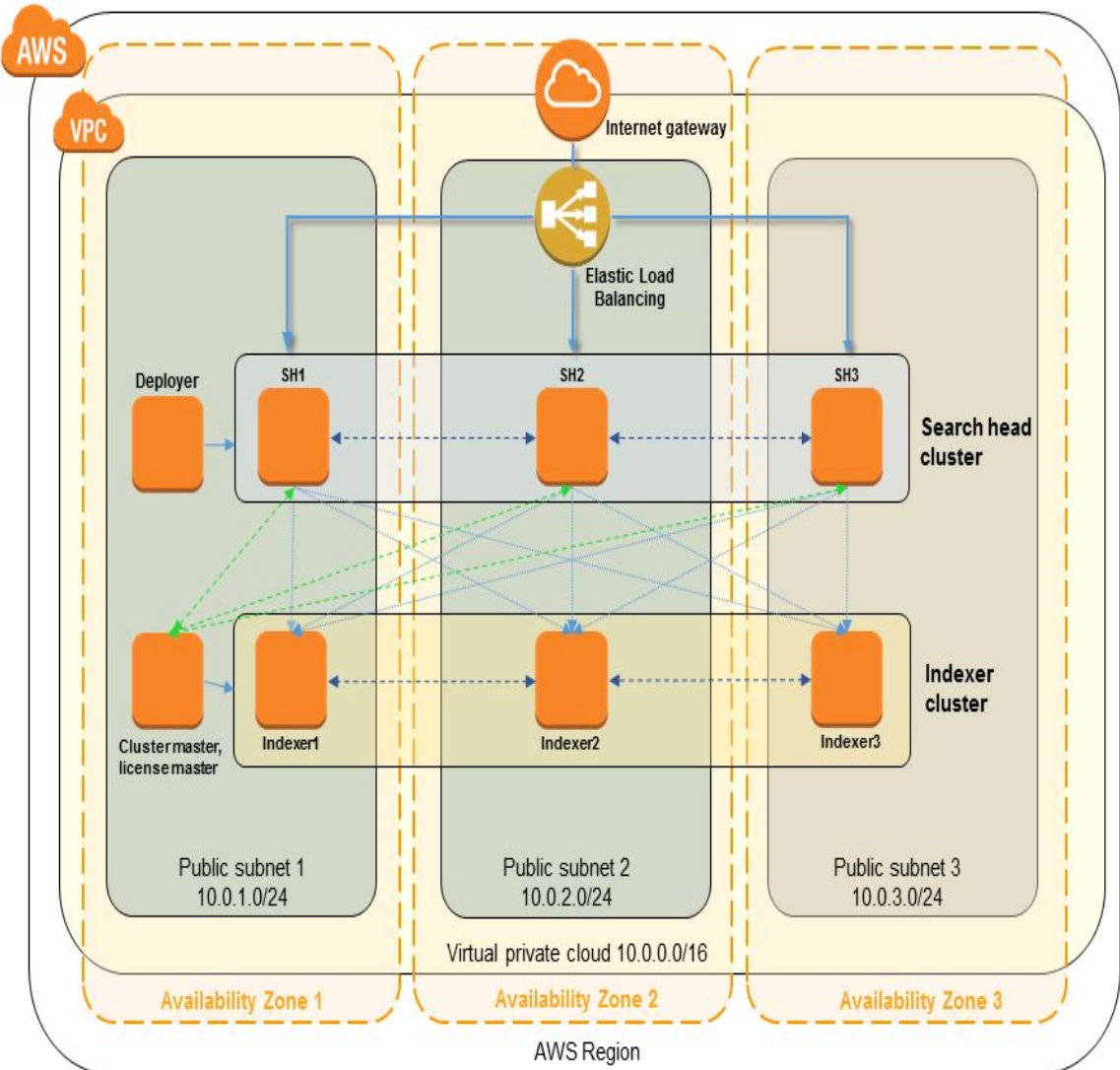
When using Splunk premium solutions, such as Splunk® Enterprise Security (ES) or Splunk® IT Service Intelligence (ITSI), we recommend indexer instance types with a larger memory footprint.

Storage Selection Examples

| SPLUNK | | | AWS |
|--------------|--|------------|------------------------------|
| Bucket Stage | Description | Searchable | Storage Option |
| Hot | Contains newly indexed data. Open for writing. One or more hot buckets for each index. | Yes | EBS gp2 Instance Storage* |
| Warm | Data rolled from hot. There are many warm buckets. Warm buckets are read-only. | Yes | EBS gp2 Instance Storage* |
| Cold | Data rolled from warm. There are many cold buckets. Cold buckets are read-only. | Yes | EBS gp2 EBS st1 or sc1 |
| Frozen | Data rolled from cold. The indexer deletes frozen data by default, but you can also archive it. Archived data can later be thawed. | No | S3 Glacier |

Splunk AWS QuickStart (IDR only) – Splunk in 45 mins

- Splunk indexer cluster with the number of indexers you specify (3-10)
- Splunk search heads, either stand-alone or in a cluster
- Splunk license server and indexer cluster master
- Splunk search head deployer
- (Optional) User-provided Splunk apps and/or add-ons



Real-Time Data Analytics, IT Monitoring & Troubleshooting

A FINRA case study



Company overview

FINRA - the Financial Industry Regulatory Authority - is the largest independent regulator for all securities firms doing business in the United States. FINRA's mission is to protect investors by making sure the US securities industry operates fairly and honestly.

Up to **99B**

Financial transactions
monitored every day

1,369

Fraud cases referred to
the SEC (U.S. Securities
and Exchange
Commission) in 2017

\$66.8M

Restituted to harmed
investors in 2017

Challenges

FINRA needed to integrate its processes into a DevSecOps workflow in order to keep up with the constantly evolving security industry.

It was determined that FINRA previously lacked:

- An automation pipeline for both its operational workflow and security posture
- A way to effectively stay ahead of compliance guidelines and security best practices
- The ability to scale up and down at any time, to match surges in compute and storage capacity needs

More data & analytics on AWS than anywhere else



Splunk is available in AWS Marketplace

Options for Splunk Cloud & Splunk Enterprise

AWS Marketplace Ease of Sale

- Easily discover & deploy software & SaaS
- **Simplified buying process** and consolidated AWS Billing reduces time to procure
- **Automatic renewals**
- One consolidated AWS bill
- Potential impact and “draw-down” on AWS **EDP (Enterprise Discount Program) Contracts**



[Explore AWS Marketplace](#)

Splunk Specifics

- Annual contract subscriptions & automatic discount for multi-annual options
- Buy Splunk Cloud in **increments of 5GB to 100GB** across all supported regions
- Easily upgrade Splunk license
- **Marketplace seller private offers** available for larger index volumes, apps and add-ons
- **Splunk Enterprise licensing** available via AWS Marketplace seller **private offers**

New! [Splunk Insights for Infrastructure Pay-as-You-Go](#)

The AWS & Splunk solution

FINRA has been able to bridge the gap between its security and operations teams.

FINRA:

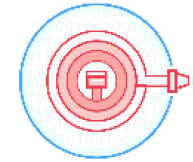
- Moved into serverless computing environment on AWS
- Started leveraging AWS Lambda to run code without provisioning or managing servers
- Began ingesting and logging more data than ever from over 170 applications
- Integrated Amazon Kinesis Data Firehose to deliver real-time streaming data to Splunk

“**The insights from Splunk allow us to use more AWS services.** We are putting our crown jewels — our ability to take every transaction every day on almost every U.S. stock and options market and analyze that data in the cloud — and we are using Splunk to assure that it is secure. **Splunk and AWS together give us an unparalleled ability to protect investors.**”

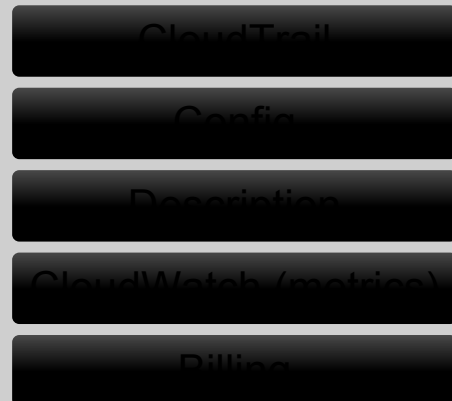
Gary Mikula, Director, Cyber and Information Security, FINRA

Getting Data from AWS

Heavy Forwarder



Legacy (API Pull)



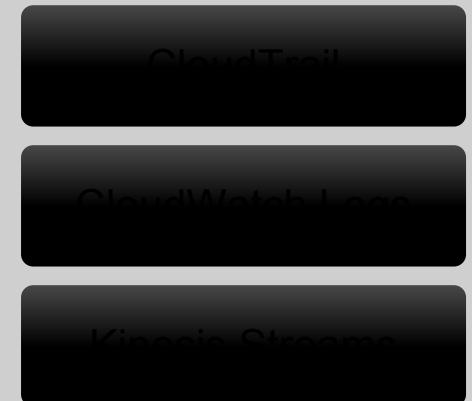
SQS Based S3



Lambda



Kinesis Firehose



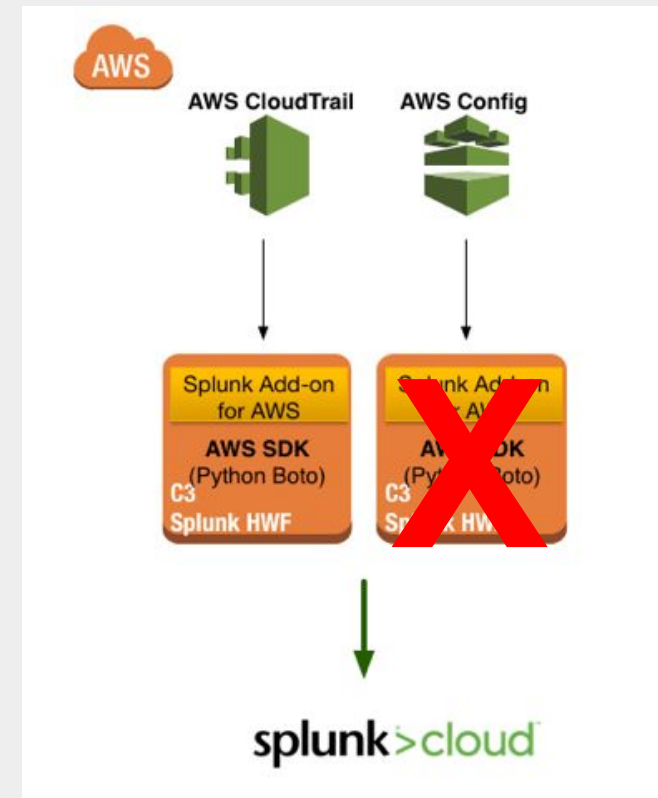
Server

Serverless

Architecture Tips

Splunk – SQS based S3 vs. Legacy Modular Input

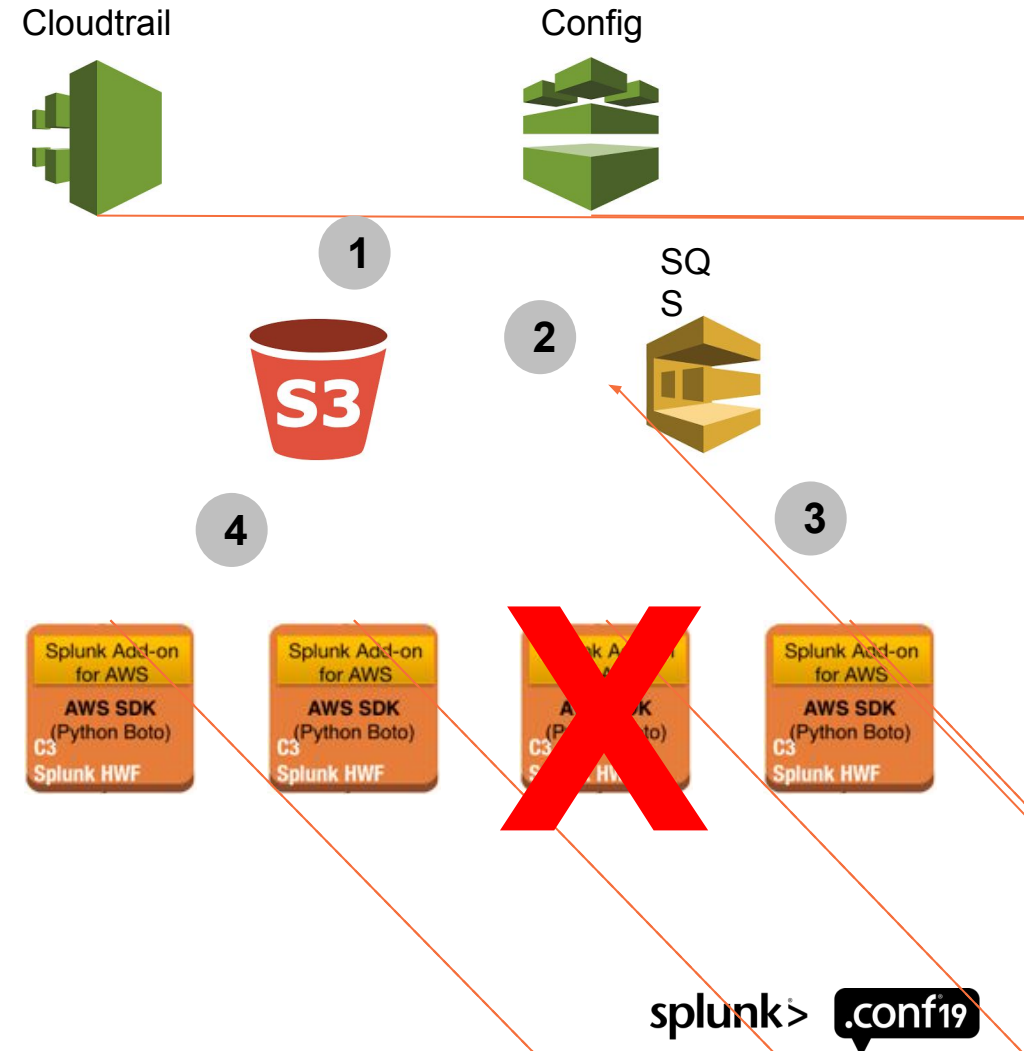
- Legacy Modular Input does not have fault tolerance. If one HWF goes down, then it can no longer collect the data and send it to get indexed
- Each HWF must maintain state, which means that upon failure you will have to move the input to another working node
- The data collection cannot be load balanced across tiers



SQS Based S3 vs. Legacy Modular Input

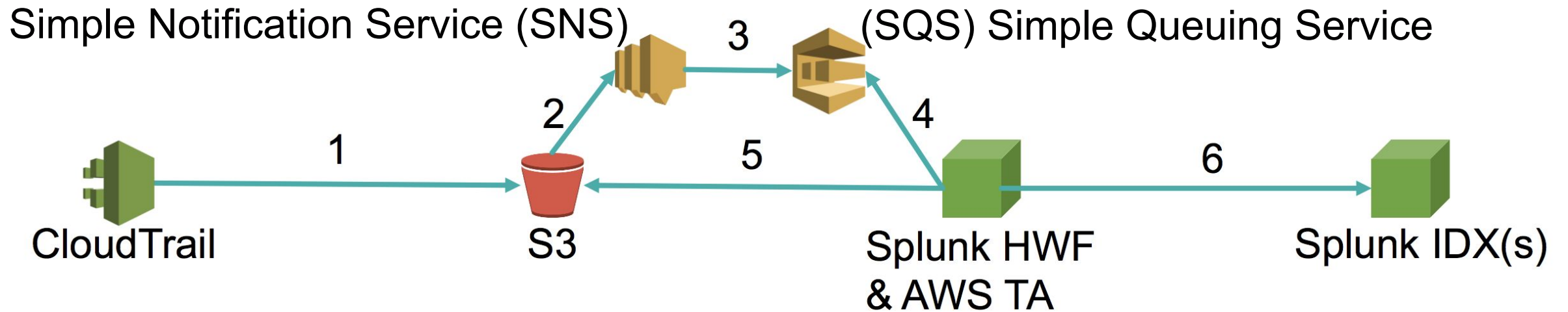
SQS Based S3 input is a more scalable approach to collect AWS Data

- Fault tolerant data collection. If one node fails, another node will collect the data.
- Once data is in S3, event is posted to SQS. Any of HWF can then pickup SQS Msg and get data.
- Each HWF is stateless and will not impact the data collection from any other node.
- Data collection can be load balanced across multiple heavy forwarder nodes.



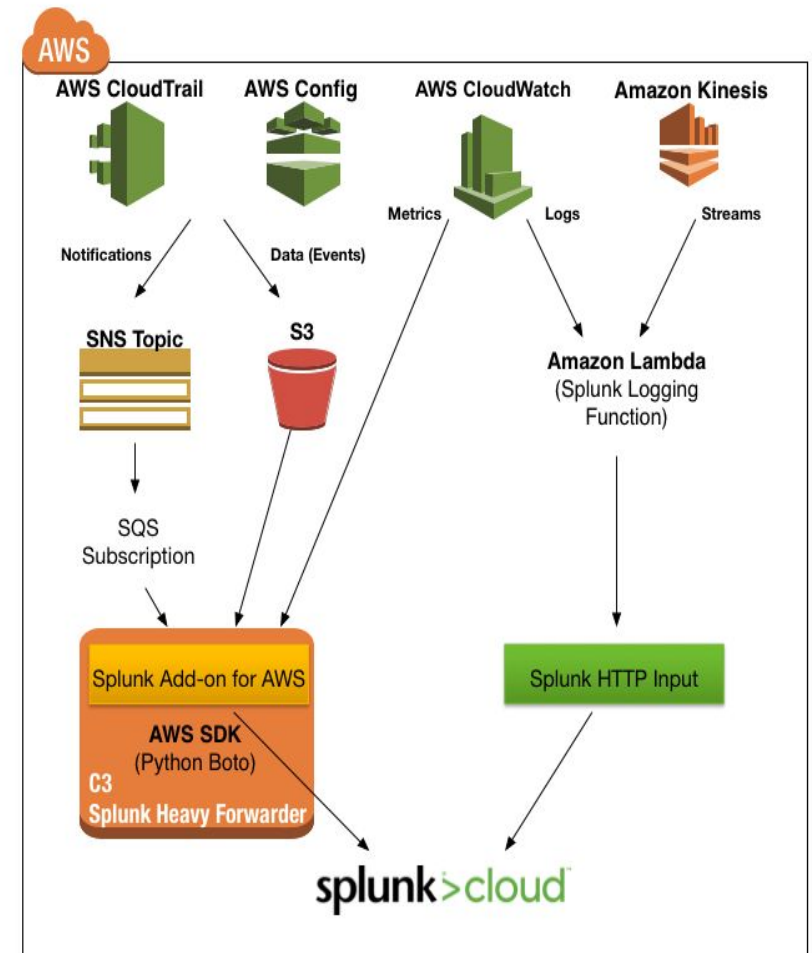
SQS-Based S3

Example Flow



General guidance when collecting AWS Data

- Collect AWS data using a Splunk Heavy Forwarder for SQS Based S3 and other modular inputs (Billing, Inspector, Config Rules, Description etc.) (Managed in Splunk Cloud)
- Collect high volume data using Lambda Function to Splunk HTTP Event Collector (HEC)
- Kinesis Firehose can collect data in real-time with a built in buffer plus a “splash back” to an S3 bucket.



Trumpet 2.0

Automated AWS Configuration for Splunk Add-On

General configuration
Provide general details about your AWS and Splunk environment.

Splunk endpoint URL and port [?](#)
Example: https://1.1.1.1:8080

HTTP Event Collector Token (Indexer acknowledgement enabled) [?](#)
For example: 12345678-9abc-def0-123456789abc

AWS data source configuration
Select the AWS data sources which will be sent to Splunk

☒ AWS Config Notifications ☐
☒ AWS Config Snapshots ☐
☒ AWS CloudTrail ☐
☒ AWS VPC Flow logs ☐
☒ AWS CloudWatch logs ☐
☒ AWS CloudWatch Events ☐ Select...

[Download CloudFormation template](#)



Firehose delivery streams

Kinesis Firehose delivery streams continuously collect, transform, and load streaming data into the destinations that you specify.

[Create delivery stream](#) [Test with demo data](#) [Delete](#)

Filter or search by name

| | Name | Status | Created | Source | Record transformation | Destination |
|-----------------------|--|--------|-----------------------|-------------------|-----------------------|-------------|
| <input type="radio"/> | splunk-trumpet-cwefirehosedeliverystream- | Active | 2018-10-31T11:53-0700 | Direct PUT and... | splunk-trumpet... | Splunk |
| <input type="radio"/> | splunk-trumpet-flowlogs-vpcfiredeliverystream- | Active | 2018-10-31T12:30-0700 | Direct PUT and... | splunk-trumpet... | Splunk |

Viewing 1 - 2 of 2 delivery streams

AWS Console



| Values | Count | % |
|----------------------------|-------|--------|
| aws:cloudtrail | 9,197 | 92.33% |
| aws:cloudwatchlogs:vpcflow | 735 | 7.379% |
| aws:config:notification | 11 | 0.11% |
| aws:guardduty:firehose | 10 | 0.1% |

Splunk



- [AWS API Call Events](#)
- [AWS Management Console Sign-in Events](#)
- [Amazon EC2 Events](#)
- [AWS Systems Manager Events](#)
- [Amazon EC2 Maintenance Windows Events](#)
- [Amazon ECS Events](#)
- [Amazon GuardDuty Events](#)
- [AWS Health Events](#)
- [AWS KMS Events](#)
- [Amazon Macie Events](#)
- [Scheduled Events](#)
- [AWS Trusted Advisor Events](#)

Trumpet 2.0 Cloudformation Template

Dynamically generated CloudFormation sets up customized Firehose transport to Splunk

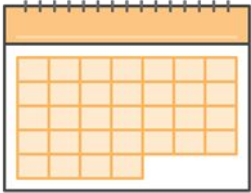
End-to-end visibility with Splunk Cloud and AWS

A PagerDuty case study

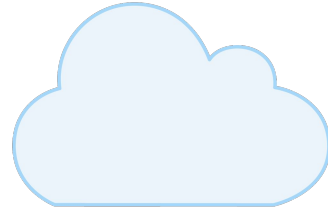




PagerDuty-at-a-Glance



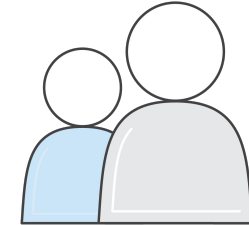
Founded in 2009



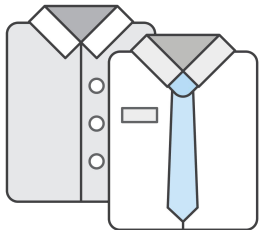
Cloud-based incident resolution



Based in San Francisco



200,000+ Users



9,000+ customers
Startups to Fortune 500



Advanced Technology Partner



Quarter million incidents per day



200+ Native Integrations

PagerDuty's Security Challenge

PagerDuty needed to take a more elastic security stance to investigate and respond quickly in order to:

- Monitor and triage threats
- Maintain security posture
- Mitigate risk
- Ensure optimal customer experience and minimize service interruption
- Meet operational analysis needs

PagerDuty had previously relied on a logging solution that output data—not answers, and couldn't scale to meet the growing business needs.

The Solution – Why Splunk?

PagerDuty adopted **Splunk Cloud** running on **AWS** in order to:

- Speed incident investigations and response times
- Provide analysts with rich contextual info for informed decision-making
- Mitigate risk
- Provide high availability of its services
- Scale to meet customer demand as needed
- Reduce cost by 30% over previous solution

Splunk is available in AWS Marketplace

Options for Splunk Cloud & Splunk Enterprise

AWS Marketplace Ease of Sale

- Easily discover & deploy software & SaaS
- **Simplified buying process** and consolidated AWS Billing reduces time to procure
- **Automatic renewals**
- One consolidated AWS bill
- Potential impact and “draw-down” on AWS **EDP (Enterprise Discount Program) Contracts**



[Explore AWS Marketplace](#)

Splunk Specifics

- Annual contract subscriptions & automatic discount for multi-annual options
- Buy Splunk Cloud in **increments of 5GB to 100GB** across all supported regions
- Easily upgrade Splunk license
- **Marketplace seller private offers** available for larger index volumes, apps and add-ons
- **Splunk Enterprise licensing** available via AWS Marketplace seller **private offers**

New! [Splunk Insights for Infrastructure Pay-as-You-Go](#)

Enterprise-wide Visibility and High Availability

- Security**

Ensures product security; fast time to investigate, minimizes risk and downtime

- Compliance**

Automated daily searches ensure compliance across a range requirements with no manual intervention

- Operations**

Delivers on goal of being one of most highly available services worldwide

- Application Development**

Enables DevOps/ Distributed Operations with real time visibility into production environments

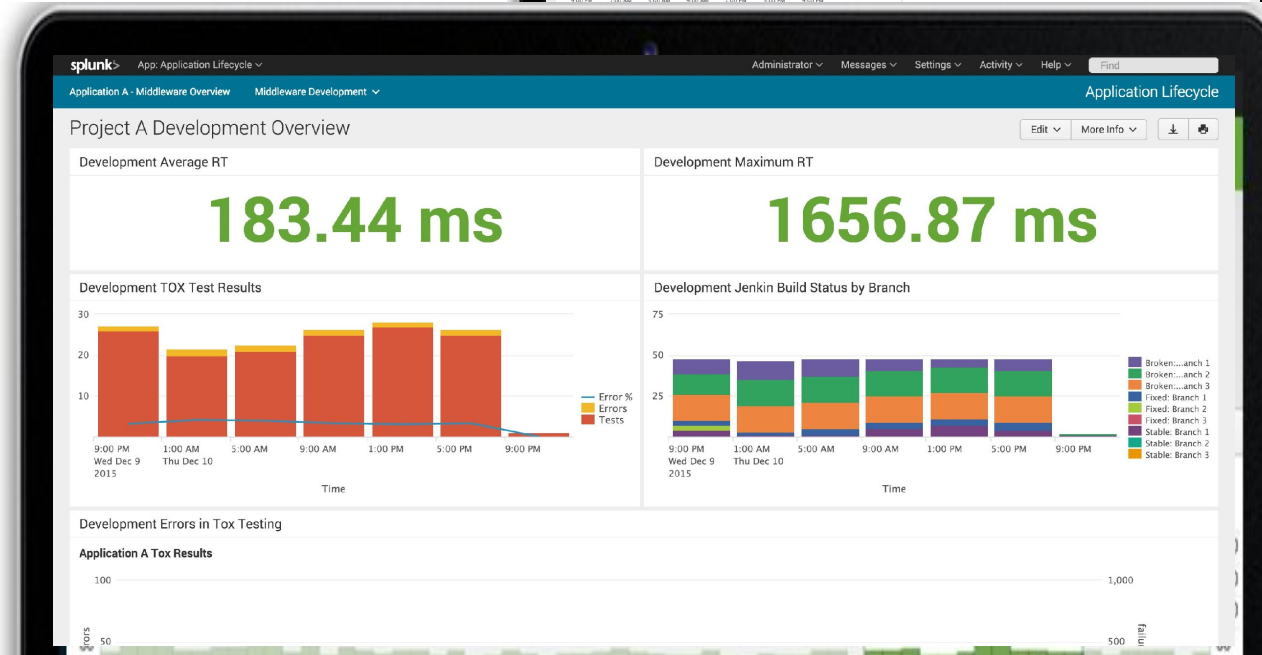
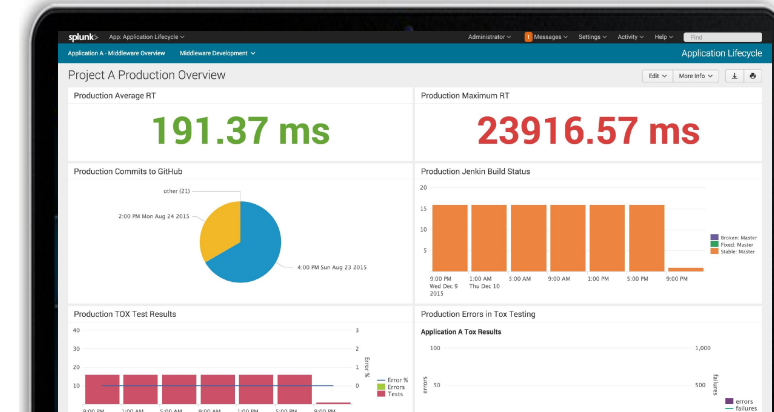


Enhancing Security and Compliance

- Prior solution provided data...but not answers
- Made our security program more effective and easier to run
- Threshold-based alerts helps minimize alert fatigue, prioritize investigations
- Dashboards quickly pinpoint anomalies warranting further investigation
- Eliminates need for disparate tools
- AWS App provides change mgt./change tracking audit trail for compliance

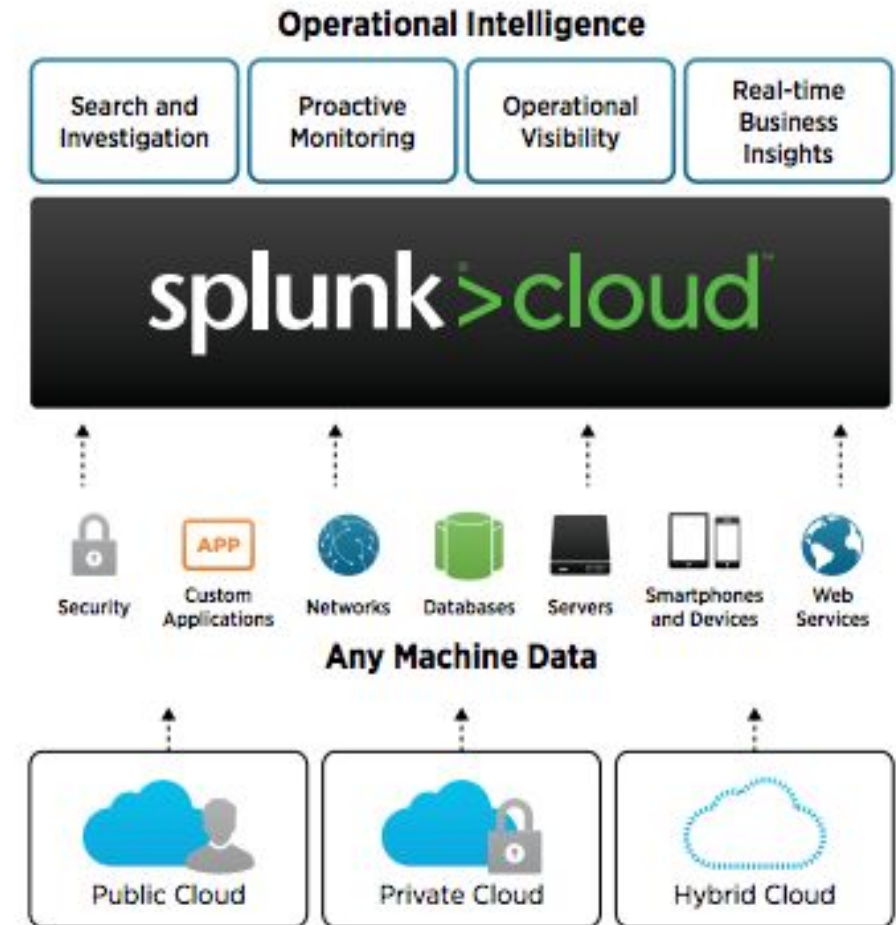
Powering Engineering and Distributed Operations

- Delivering new product securely with speed and agility
- Historical trending helps team understand where to invest energy
- Keep engineering resources focused on running the business and customer satisfaction versus tools maintenance



Business Analytics and Beyond

- Finance team using platform for visibility into customer usage trends
 - Leading indicator of renewals/ at-risk accounts
- Execs and Product Management use Splunk for view into overall business health



Summary of Results

PagerDuty deployed **Splunk Cloud** as its platform for operational visibility and triage across the business—from IT operations monitoring to security and compliance.

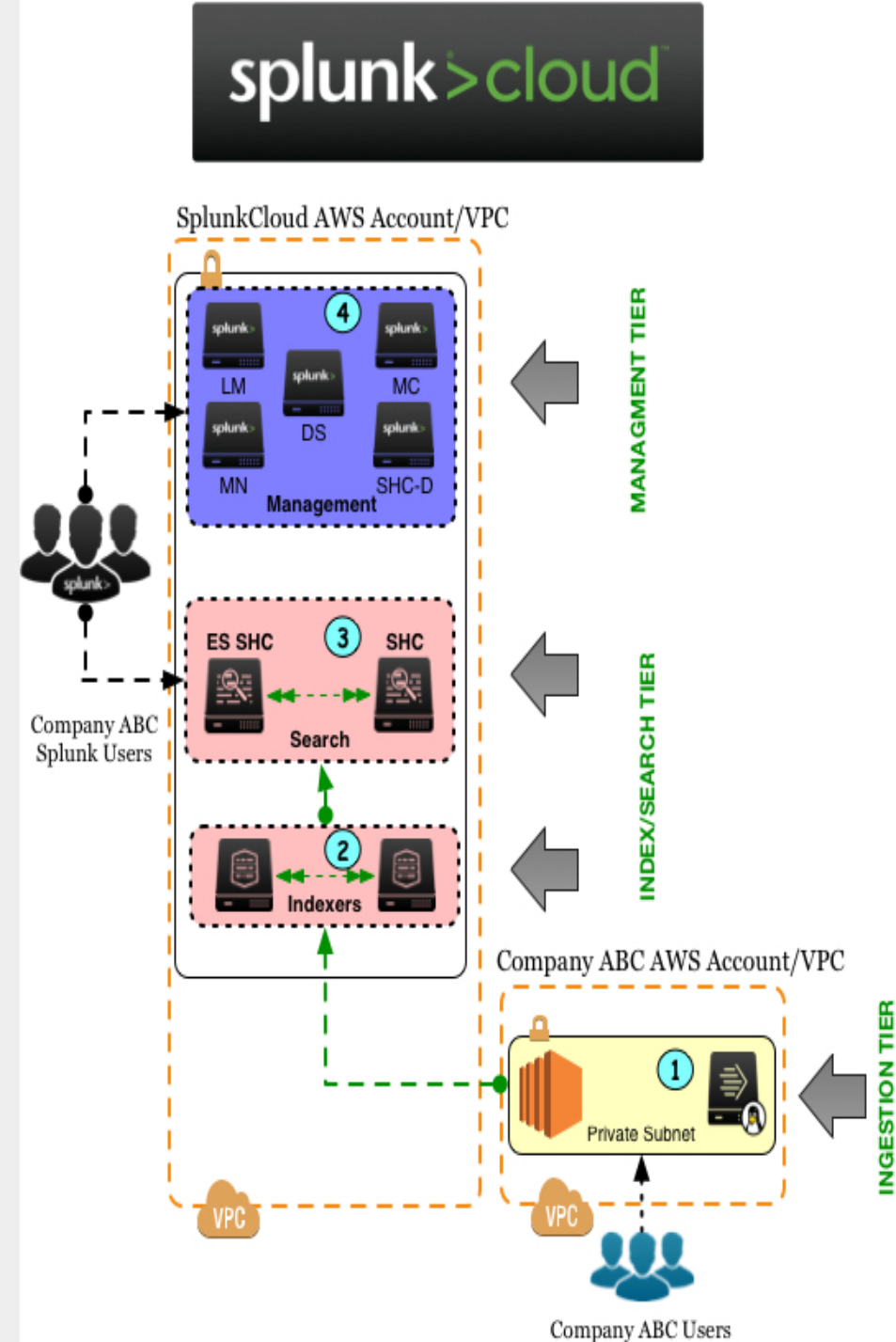
With Splunk Cloud, Engineering has a solution for monitoring and alerting, and then can dig deeper into the source of issues and resolve them quickly.

- Ensured customer satisfaction and highly available cloud services
- Reduced IT & security incident resolution from hours to minutes & seconds
- Realized 30% cost savings over prior service

Architecture Tips

SplunkCloud - SaaS

- You only have one Primary Concern: Send data to SplunkCloud which runs in Splunk's AWS Account.
- Data can be sent to Splunk Cloud using a Splunk forwarder (Universal Forwarder).
- You can use the REST API, HEC, and SDKs with Splunk Cloud.



Managing Splunk Is More Than Just Software

| | Responsibility | Splunk Ent Deployed On-Premises | Splunk Ent BYOL Deployed on AWS | Splunk Cloud |
|--------------------------------------|--|------------------------------------|------------------------------------|-----------------|
| Admin tasks: One-time setup | Purchase/rent HW | Customer | AWS | Splunk |
| | Rack and stack, cable, network all HW | Customer | AWS | Splunk |
| | Install Splunk | Customer | Customer | Splunk |
| | Install OS | Customer | AWS* | Splunk |
| | Configure Splunk (create users, load apps, configure | Customer | Customer | Splunk |
| | Configure indexes | Customer | Customer | Splunk |
| | Setup HA/clustering | Customer | Customer | Splunk |
| | Setup disaster and recovery | Customer | Customer | Splunk |
| | Configure forwarders | Customer | Customer | Joint |
| | Onboard data | Customer | Customer | Joint |
| | Integrate with LDAP/AD | Customer | Customer | Joint |
| Admin tasks: ongoing | Scale up HW | Customer | Customer | Splunk |
| | Install Splunk patches / upgrades | Customer | Customer | Splunk |
| | Install OS patches / upgrades | Customer | Customer | Splunk |
| | Monitor deployment / health checks | Customer | Customer | Splunk |
| | Manage forwarders | Customer | Customer | Customer |
| | Create users / roles | Customer | Customer | Customer |
| | Manage indexes | Customer | Customer | Customer |
| | Onboard additional data | Customer | Customer | Customer |
| | Load search head only apps | Customer | Customer | Splunk |
| | Load distributed apps | Customer | Customer | Splunk |
| | Load premium apps | Customer | Customer | Splunk |
| | Export data | Customer | Customer | Splunk |
| User tasks | Search, alerts, reports, dashboards | Customer | Customer | Customer |

AWS Marketplace

A brief overview

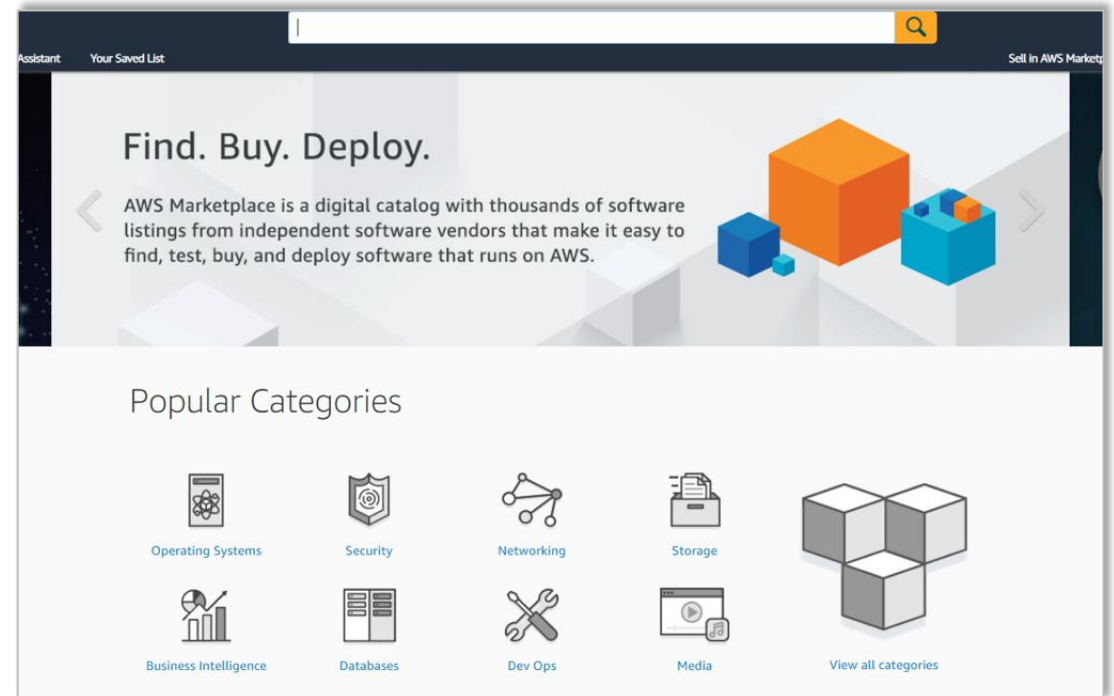


A growing digital software catalog


























- Deploy software on demand
- **1,400+** ISVs
- **300** Security ISV's
- Over **4,800** product listings
- **200,000** active customers
- **100,000** + active security subscriptions
- Over **650 million** hours of EC2 deployed monthly
- Deployed in **18 regions**
- Offers **39 categories**



- Flexible consumption and contract models
- Easy and secure deployment, almost instantly
- One consolidated bill
- Always evolving




Largest ecosystem of security partners and solutions

| Infrastructure security | Identity & access control | Configuration & vulnerability analysis | Logging & monitoring |
|---|--|---|---|
|             |    <p data-bbox="1054 868 1291 973">Data protection</p> |             |     |

Demo

 **Services** ▾ **Resource Groups** ▾ 

 AdminiRole/ialek-Isengard @ 5... ▾ N. Virginia ▾ Support ▾

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

6. Configure Security Group

7. Review

Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start (0)

My AMIs (0)

AWS Marketplace (14)

Community AMIs (32)

Categories

All Categories

splunk>enterprise

Splunk Enterprise

★★★★★ (12) | 7.3.2 [Previous versions](#) | By [Splunk Inc.](#)

Bring Your Own License + AWS usage fees

Free tier eligible

Linux/Unix, Amazon Linux 2018.03 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 10/10/19

The Splunk Enterprise AMI accelerates the speed at which organizations deploy Splunk Enterprise in AWS. Splunk Enterprise is the leading platform for Operational Intelligence, ...

[More info](#)

Select

Flexible software build and delivery

AWS Marketplace deployment options

Amazon Machine Image



- Ideal for single instance solutions deployed directly into customer's VPC
- You can offer customers maximum flexibility with BYOL, pay-for-what-you-use, free trials and curated Open Source options

CloudFormation Template



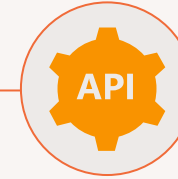
- Third-party software combined with AWS services
- You can offer complete solution implementation, including multi-instance, tie-ins to AWS Services and high-availability cluster architectures

SaaS



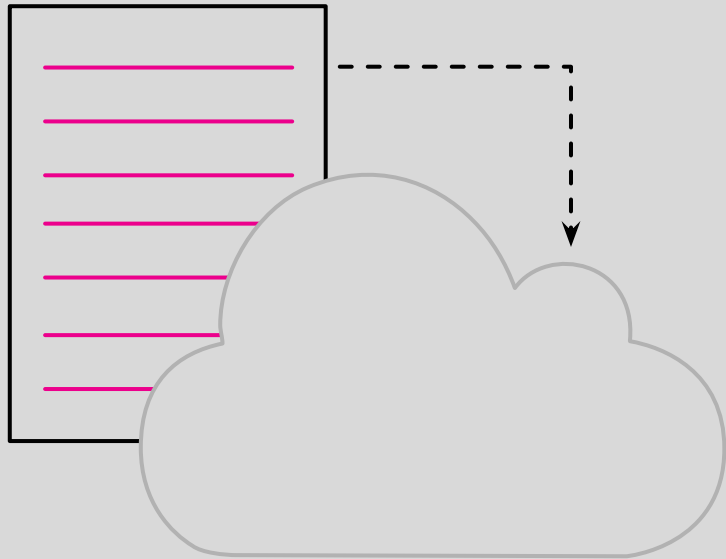
- Your SaaS solution with subscription and tiered contract options, including annual and multi-year contracts
- Enables you to integrate AWS Marketplace discovery and procurement directly to your SaaS solution

API



- Designed to integrate directly to an application
- You can offer customers high-consumption API products with simple pay-as-you-go pricing

AWS Marketplace Migration Mapping Assistant



Accelerate your migration to AWS by finding matching software in AWS Marketplace

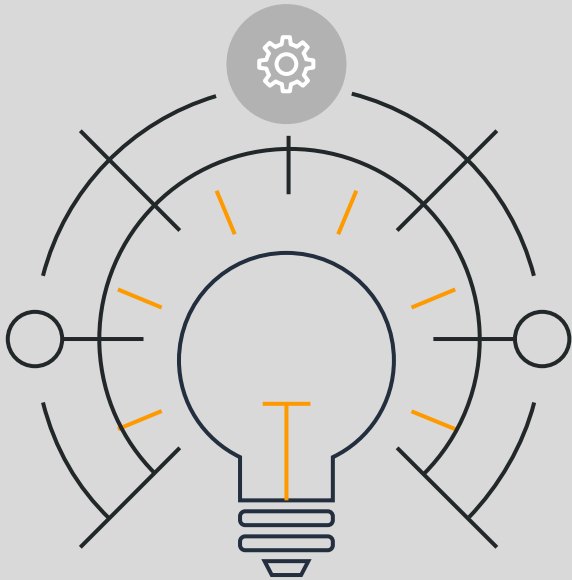
Run a bulk search and find matching software from existing inventory of on-premises applications

Software is available to purchase and deploy from AWS Marketplace

Find alternative products in the same category if matching software is not available

Always evolving

Recent innovations from



Machine Learning for
AWS Marketplace



Private
Marketplace



AWS Marketplace Seller
Private Offers



Consulting Partner Private
Offers



AWS Marketplace Flexible
Payment Scheduler



SaaS Contracts with
Consumption



AWS Marketplace for
Containers



Enterprise Contract
for AWS Marketplace



AWS Marketplace Migration
Mapping Assistant

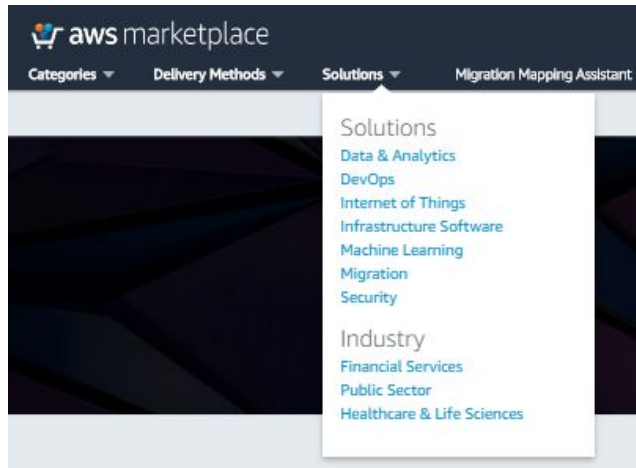


AWS Marketplace Private
Image Build (Public Beta)



Subscribe >
Configure > Launch

AWS Marketplace Solutions Finder







Security use cases


These are just a few examples of how organizations are strengthening their security posture in the cloud with AWS services and solutions in AWS Marketplace:



Structural awareness

| | | | |
|--|---|--|--|
| <p>Cloud compliance and best practices</p>  <p>Protect your cloud assets and ensure compliance with ever-changing regulatory requirements.</p> <p>Learn more»</p> | <p>Instance and container visibility</p>  <p>Gain visibility and insight into your Amazon EC2 instances and containers to protect against threats.</p> <p>Learn more»</p> | <p>Virtual private network (VPN)</p>  <p>Use a VPN to help defend against threats that put customer data and business continuity at risk.</p> <p>Learn more»</p> | <p>Secure data in AWS environments</p>  <p>Secure sensitive and highly-regulated data by encrypting entire virtual machine instances.</p> <p>Learn more»</p> |
|--|---|--|--|

Vulnerability assessment and management (VAM)



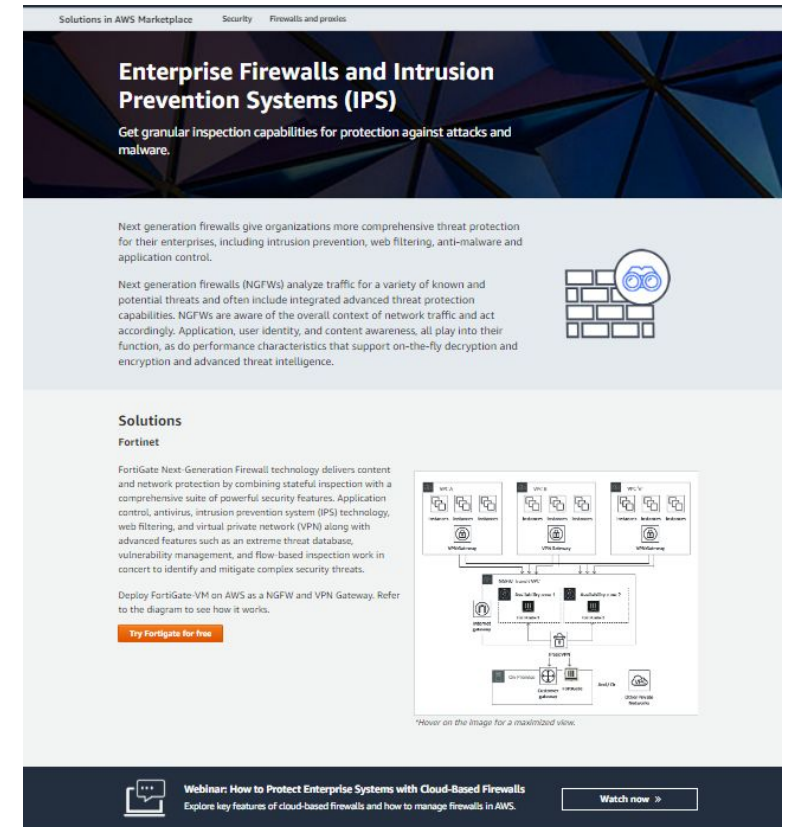
Do a one-time vulnerability assessment or establish an ongoing security management strategy.

[Learn more»](#)



Situational awareness

| | | | |
|----------------------------------|--------------------------------|---------------------------------------|--------------------------|
| Enterprise firewalls and proxies | Web application firewall (WAF) | Endpoint detection and response (EDR) | Operational intelligence |
|----------------------------------|--------------------------------|---------------------------------------|--------------------------|



Fortinet secures icare's applications in Amazon Web Services

When icare, one of the largest insurers in Australia, made their strategic decision to migrate their mission critical and customer facing applications into the cloud, they knew they had to provide the levels of security and accessibility that would give their customers, staff, and contractors complete peace of mind.

To ensure that they could deliver protection from cyber threats and a scalable platform for planned growth, they selected cloud services provider AWS to host their core insurance platform and Fortinet's FortiGate Next Generation Firewall for superior threat protection.

Key Takeaways

**It's all about
choice**

Performance-oriented
Cost-oriented

1. Splunk and AWS partner across data ingestion, cloud migration and AWS best practices to ensure joint customer success
2. Splunk provides both poll-based and streaming data ingestion options to derive IT, Security, Cost Management and IoT insights
3. You can get started with Splunk Cloud or Splunk Enterprise on AWS Marketplace.
4. Using QuickStart you can deploy reference architecture in less than an hour



**Thank
You!**