Cloud Native Monitoring at Entrust Datacard with Splunk

Daryl Robbins, Sr. Enterprise Cloud Architect, Entrust Datacard

Kara Gillis, Director of Product Marketing, Splunk

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> .conf18

Our Speakers

DARYL ROBBINS

Sr. Enterprise Cloud Architect

Entrust Datacard

KARA GILLIS

Director, Product Marketing

Splunk, IT Markets

Agenda

What We Will Cover Today

1. Intro to Splunk
2. Entrust Datacard: Who We Are
3. Creating a Unified Data Platform
4. Monitoring and Intelligent Investigations
5. Incident Management
6. Demo
7. Best Practices

What Does Machine Data Look Like?

Order Processing

Middleware Error

Care IVR

Twitter

ORDER,2014-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213. Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

---

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type 0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk T451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link: "http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place”}, objectType:"person”,preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Can't buy this device from @ACME. Site doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!”,objectType:"activity”,postedTime:"2014-05-21T16:39:40.647-0600”}

Sources

Your Machine Data is Telling a Story

Order Processing

Middleware Error

Care IVR

Twitter

Customer ID

Order ID

Product ID

ORDER,2014-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadE[illegible]uld not create pool connection. The
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused

Order ID

Customer ID

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
[illegible]98#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-
[illegible]451.16

Time Waiting On Hold

05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213

Customer ID

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:
"http://dallascowboys.com/",location:{dis[illegible]'Dallas, TX",objectType

Twitter ID

Customer's Tweet

objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Can't buy
this device from @ACME. Site doesn't work! Called, gave up on waiting for them to answer! RT if
you hate @ACME!!",objectType:"activity",postedTime:"2014-05-21T16:39:40.647-0600"}

Company's Twitter ID

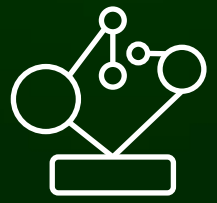
Sources

splunk>

Any Question, Any Data, In *Real Time.*

Single Platform, Many Lenses

Performance at Scale



Open Ecosystem

Hybrid

Artificial Intelligence

Finding Answers You Need to Take Action

IT Operations

How do I predict service-level degradation before it occurs?

vodafone

Application Performance Analytics

Is my poor app performance due to code-level errors or infrastructure?

UniCredit

Security and Compliance

How can I speed up security investigations and reduce the impact of insider threats?

Nasdaq

Business Analytics

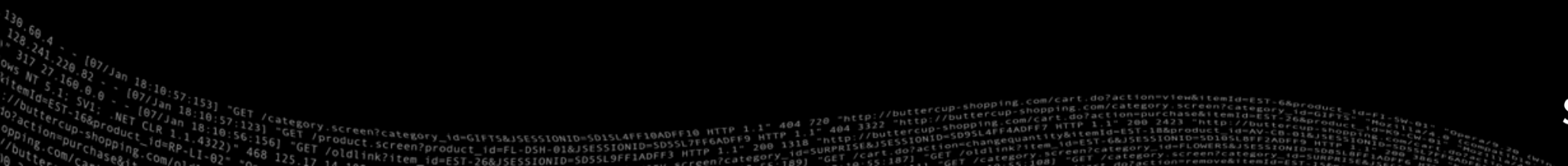
Do my marketing campaigns drive more orders through the website or mobile app?

SHAZAM

Internet of Things

How can I monitor and analyze data from tens of thousands of sensors in real time?

DB



Splunk is Trusted by Brands Around the World, Supported by a Deep Ecosystem

IT Operations	App Performance Analytics	Security & Compliance	Business Analytics	Internet of Things
intuit	NORDSTROM	BLACKROCK	Domino's	Gatwick
yelp	FamilySearch	ASU Arizona State University	UNLV	McKenney's
WORLD BANK GROUP	AAA Insurance | CSAA Insurance Group	First Data.	SHAZAM	BOSCH Invented for life
syncsort	ANSIBLE	proofpoint.	tableau	carvoyant
DELL EMC	New Relic	cisco paloalto NETWORKS	box	kepware
			TEALIUM	ThingWorx

splunkbase™

Infrastructure Monitoring Challenges

Infrastructure monitoring isn't new, but constantly changing demands require a new approach

MONITORING AND TROUBLESHOOTING IN SILOS

"Why am I monitoring with one tool and troubleshooting with another?"

INCREASING COMPLEXITY MAKES IT HARDER TO FIND AND FIX PROBLEMS

"Applications keep getting more complex and I'm required to monitor more than ever and find problems faster!"

SPENDING TOO MUCH TIME ADMINISTERING MONITORING SOFTWARE

"We don't have enough resources to buy and maintain complex monitoring tools."

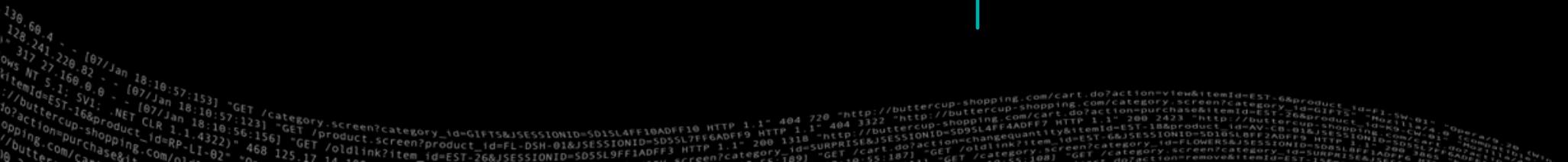
Introducing Splunk Insights for Infrastructure

Seamless metrics and logs analysis / easy to deploy and use / inexpensive

A NEW monitoring product from Splunk

splunk> insights for Infrastructure

- Collects, correlates and analyzes metrics and logs to monitor on-premises (Windows and Linux) and AWS server infrastructure
- Designed and optimized for infrastructure monitoring – from configuration to infrastructure problem investigation
- **Start FREE for small environments and inexpensively for larger environments**



What is VictorOps?

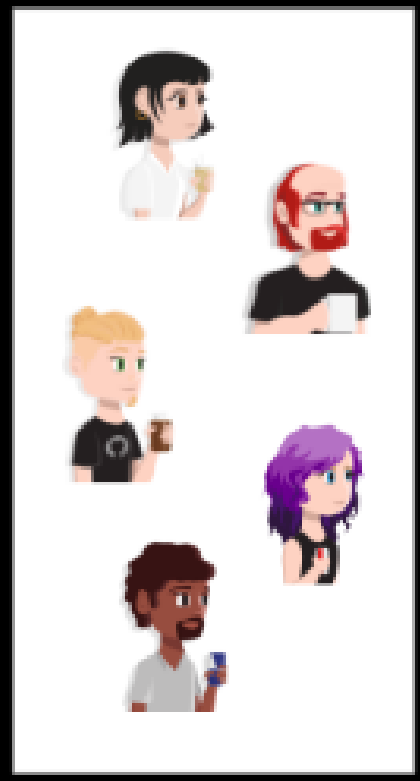
- **On-Call scheduling made simple**
- **Centralized visibility to alerts**
- **Collaborative Incident Response**
- **Post-Incident Reviews and Reporting**
- **Actionable Mobile Application**

Integrations across monitoring, CI/CD pipeline and collaboration/chat tools for a single view into alerts

VictorOps connects your software engineers with right information

When these products find broken stuff, they send the information to VictorOps

VictorOps processes the stream of event data



We engage the correct people to collaboratively solve the problem

Cloud Native Monitoring

Entrust Datacard's journey towards a Cloud Native monitoring solution with Splunk

splunk> .conf18

Entrust Datacard™

TRUST IN EVERY TRANSACTION

$600M

revenue

2,000+

employees

Sales and service in

150+

countries

34+

locations worldwide

10M+

identity and payment

credentials issued daily

Trusted Identities | Secure Transactions™

If you can trust the identity

You can trust the transaction

PRIMARY MARKETS

Payments

Digital Security

CORE CUSTOMER SEGMENTS

CONSUMER
Revolutionize the Consumer Experience

CITIZEN
Connect Citizens & Governments

ENTERPRISE
Secure Your Place in the Cloud

INTELLITRUST OFFERING

PURPOSE-BUILT SaaS PRODUCT

AWS public cloud
Agile development
Multi-tenant, multi-tier

SaaS BUSINESS MODEL

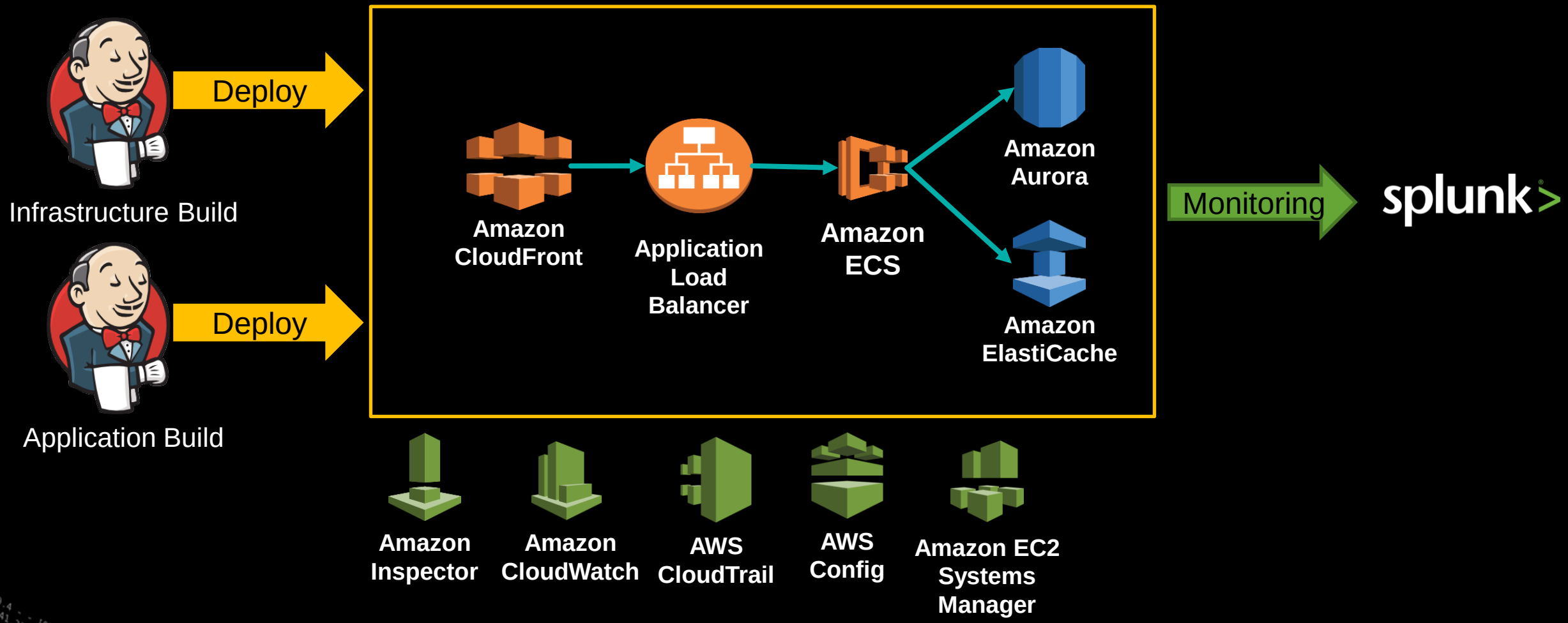
Trial capabilities, easy onboarding
Frictionless user experiences
Flexible & dynamic — subscription pricing

- Per User
- Per Transaction

REPUTATION FOR SECURITY & IDENTITY

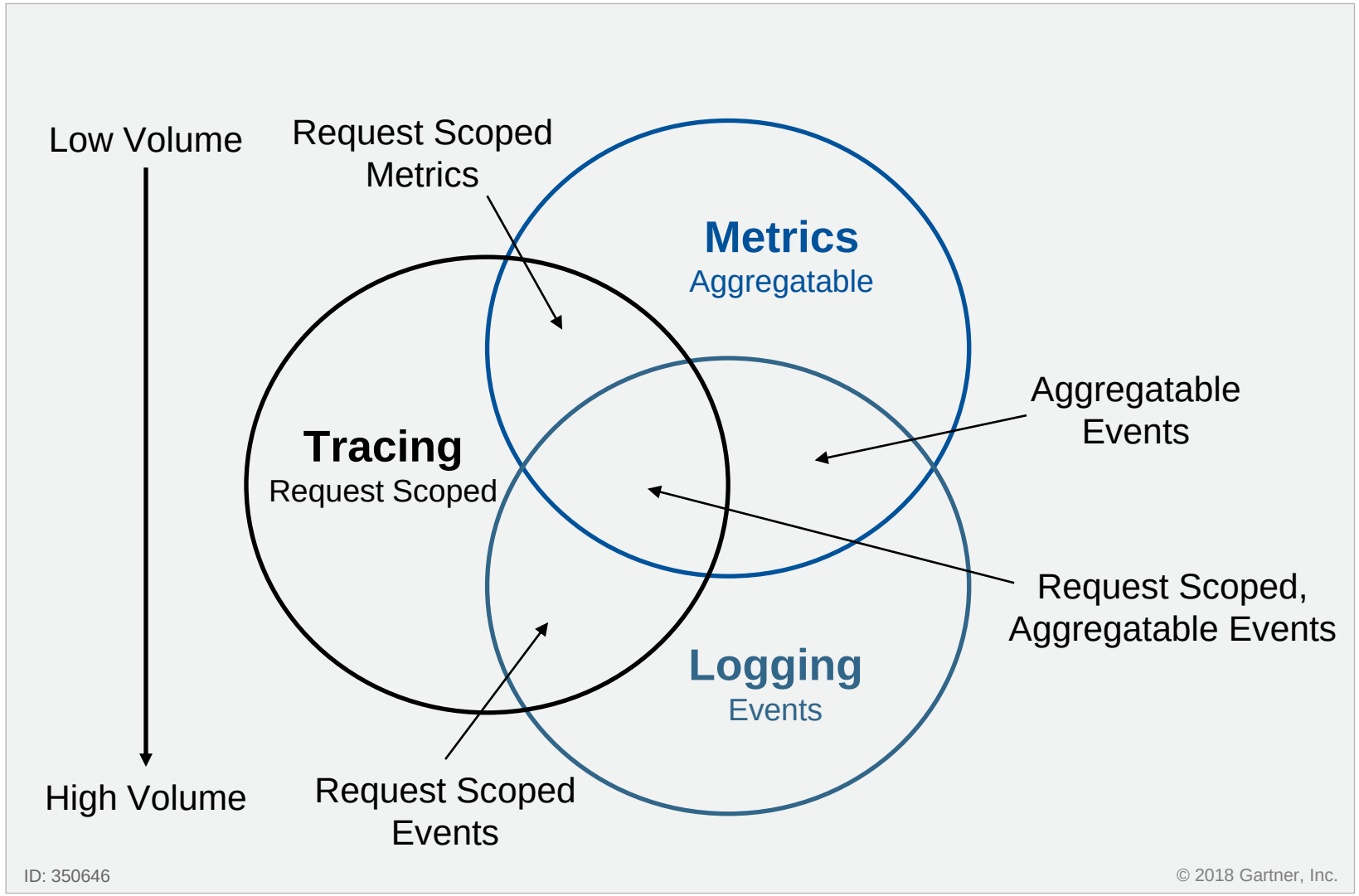
Security & identity in our DNA
Leverage learnings of IDG
High-assurance use cases
Enterprise complexity

IntelliTrust™ Architecture



Pillars of Observability

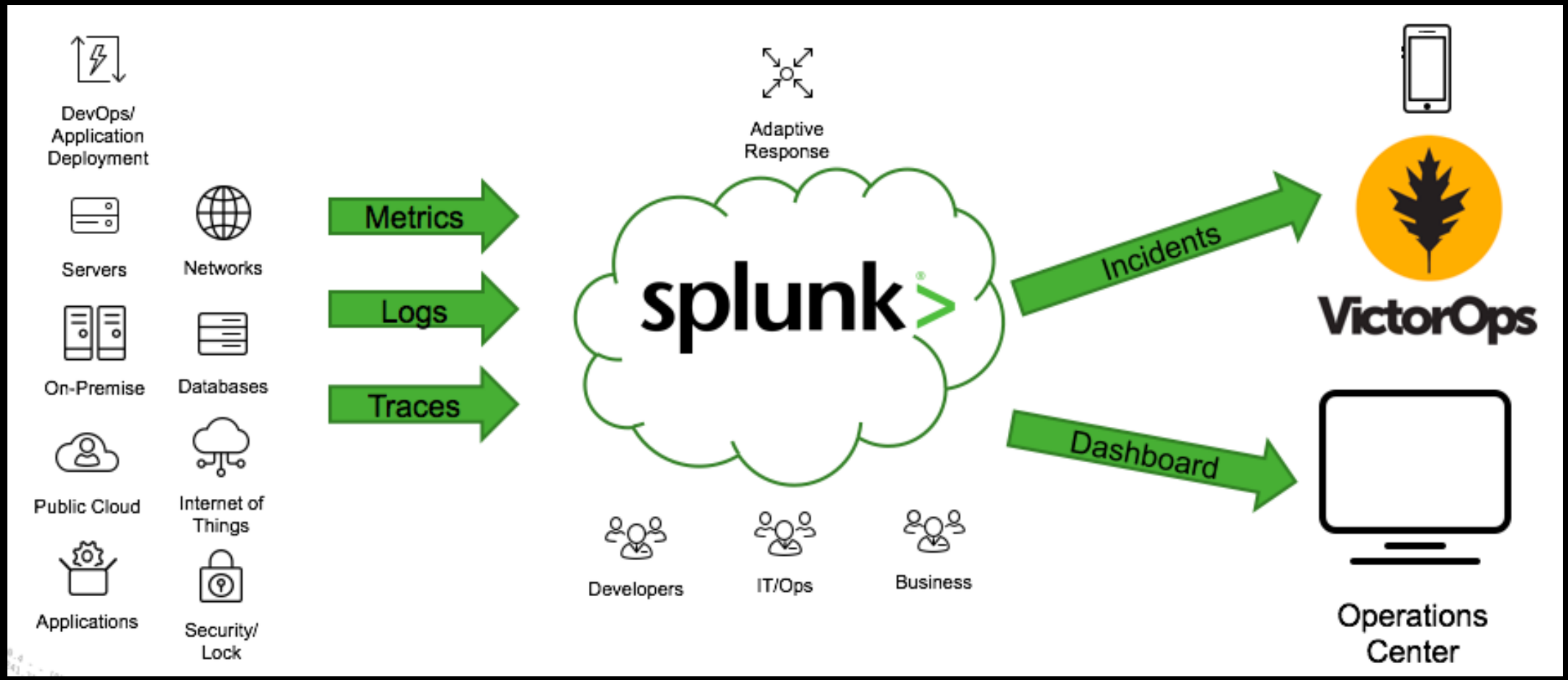
Types of Monitoring Data



Source: [Monitoring Modern Services and Infrastructure]

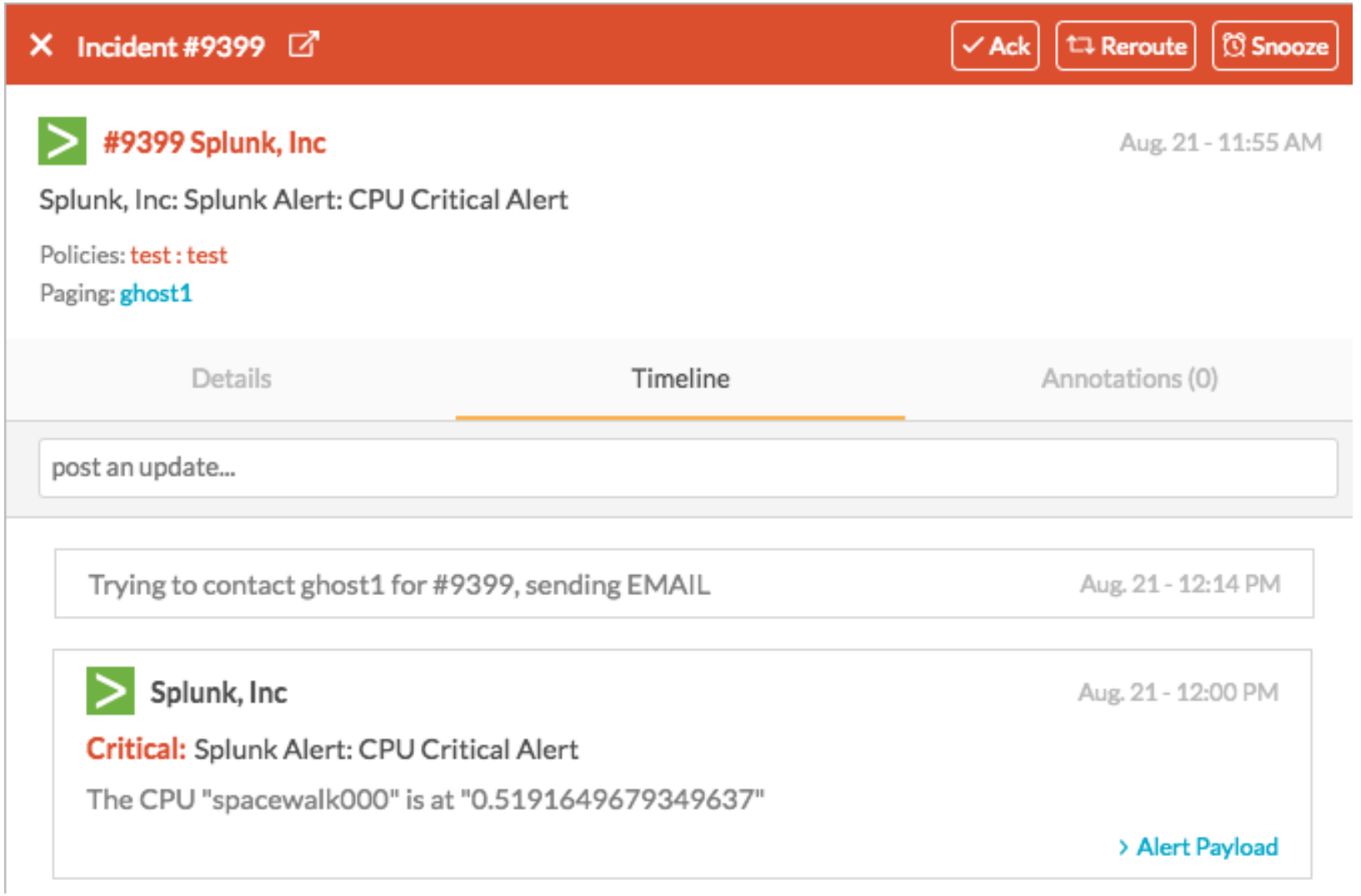
Creating a Unified Data Platform

Architecture, DevOps toolchain



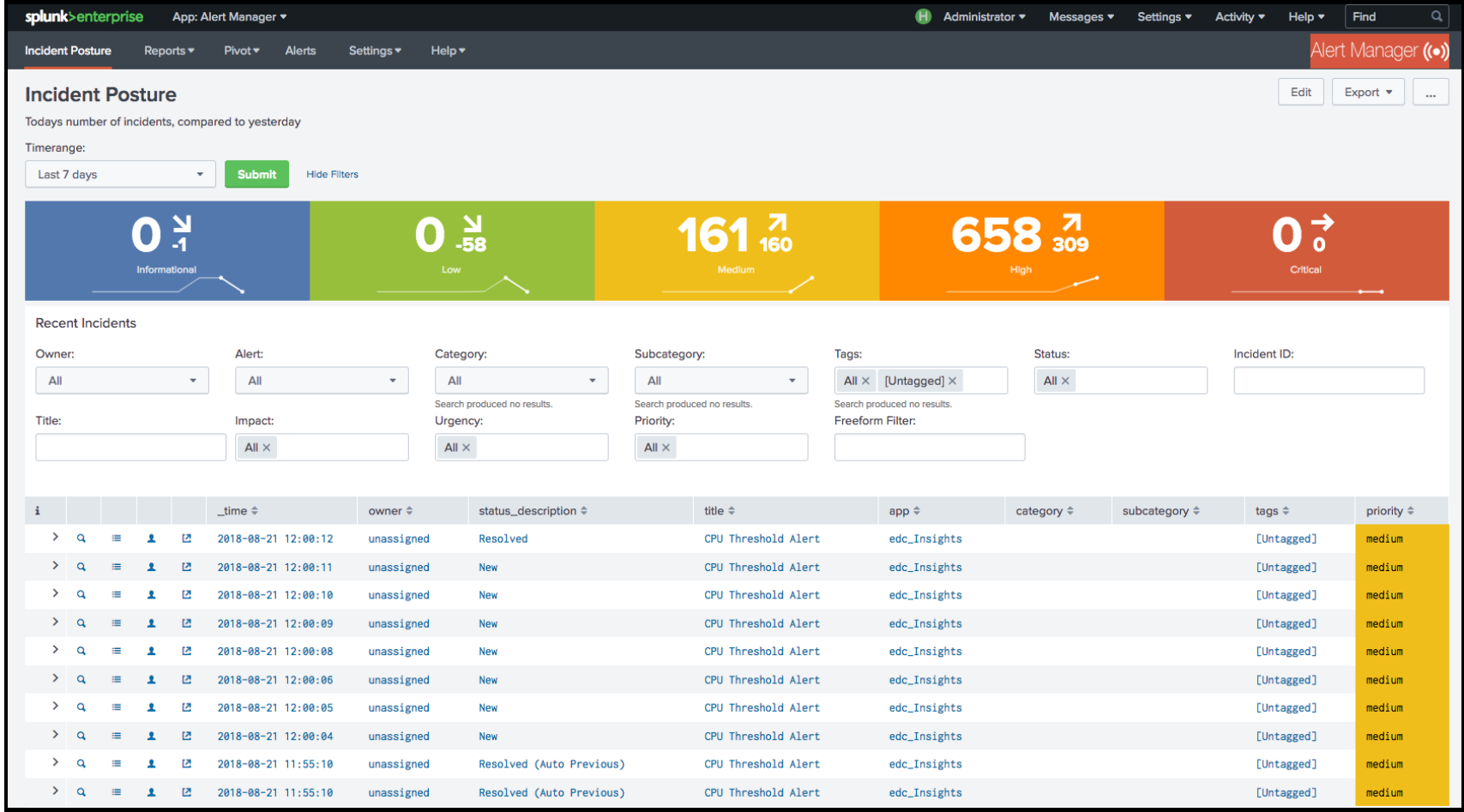
VictorOps

Incident from Splunk



App Manager

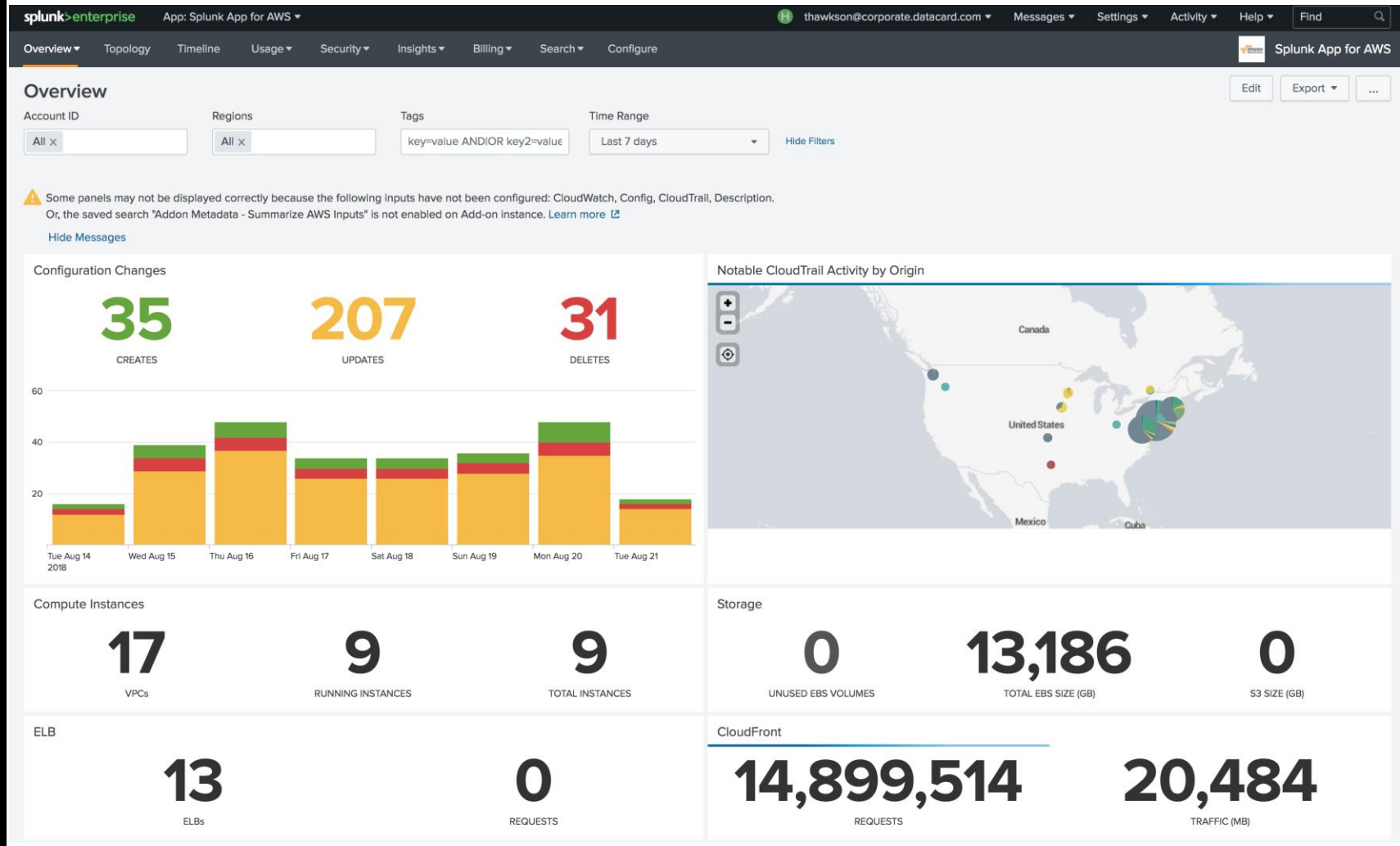
Summary of incidents

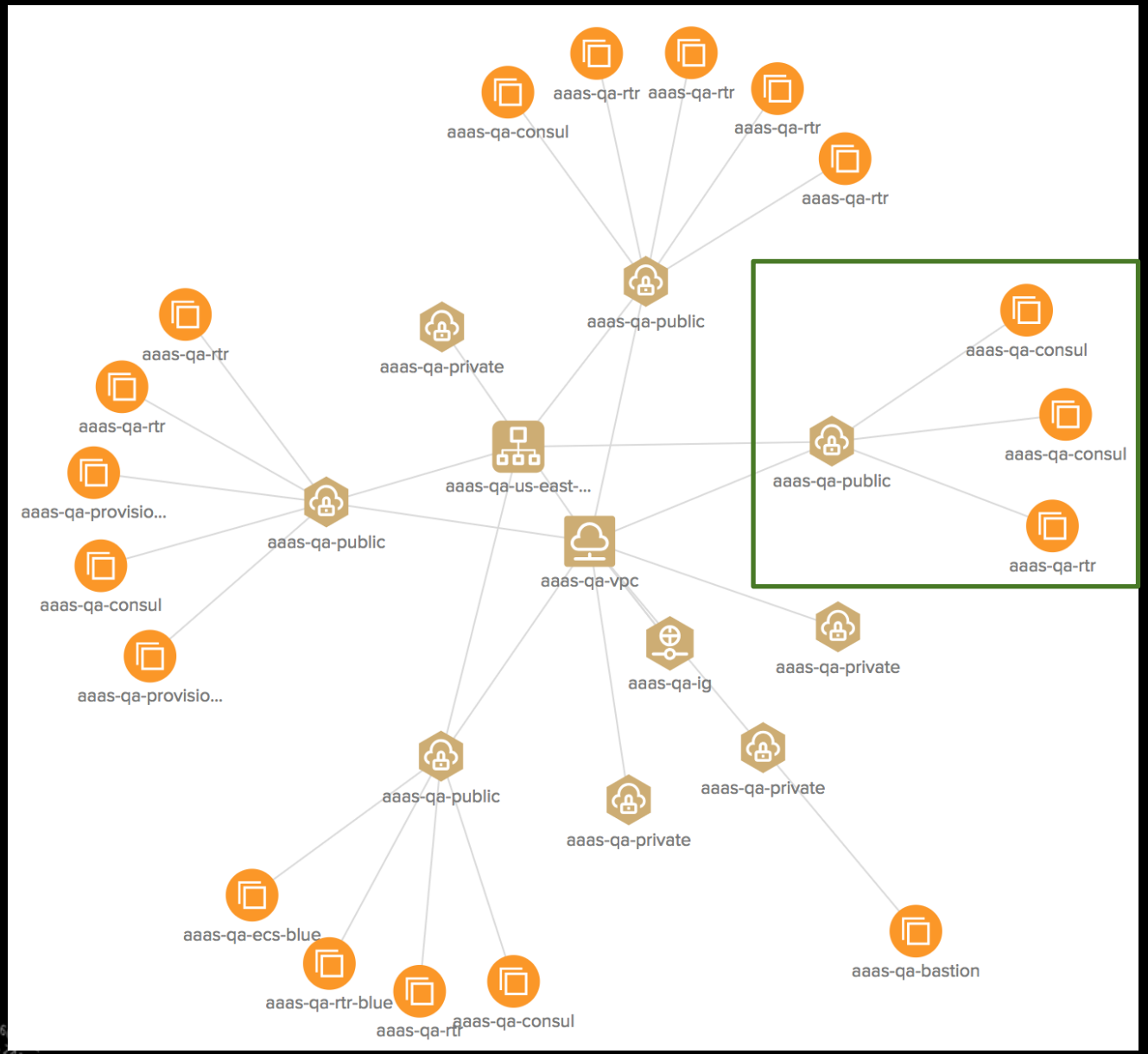


splunk> .conf18

AWS Dashboard

Overview of your account





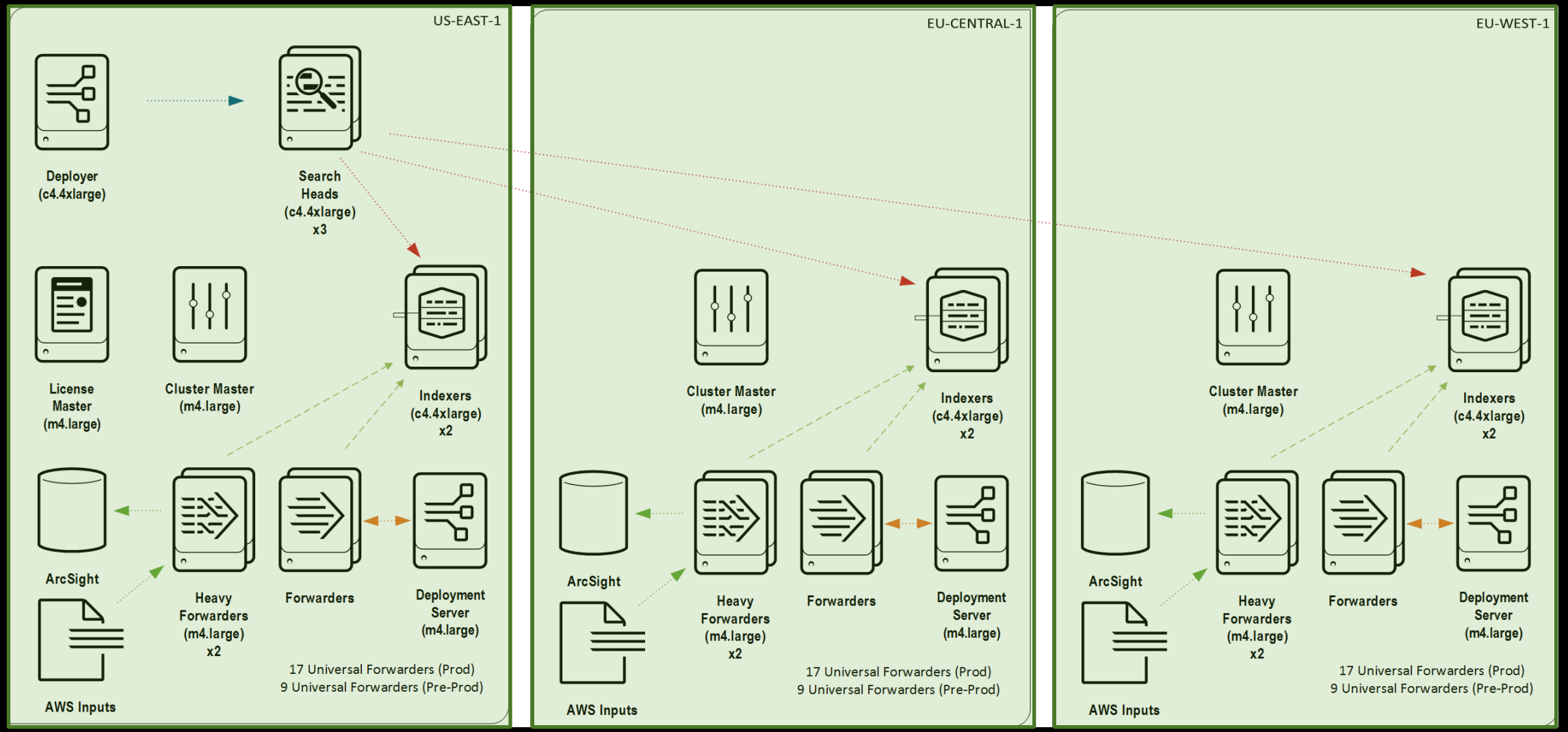
App for Infrastructure Demo

Presented by Daryl Robbins

https://youtu.be/QCvZ1Buc2VM

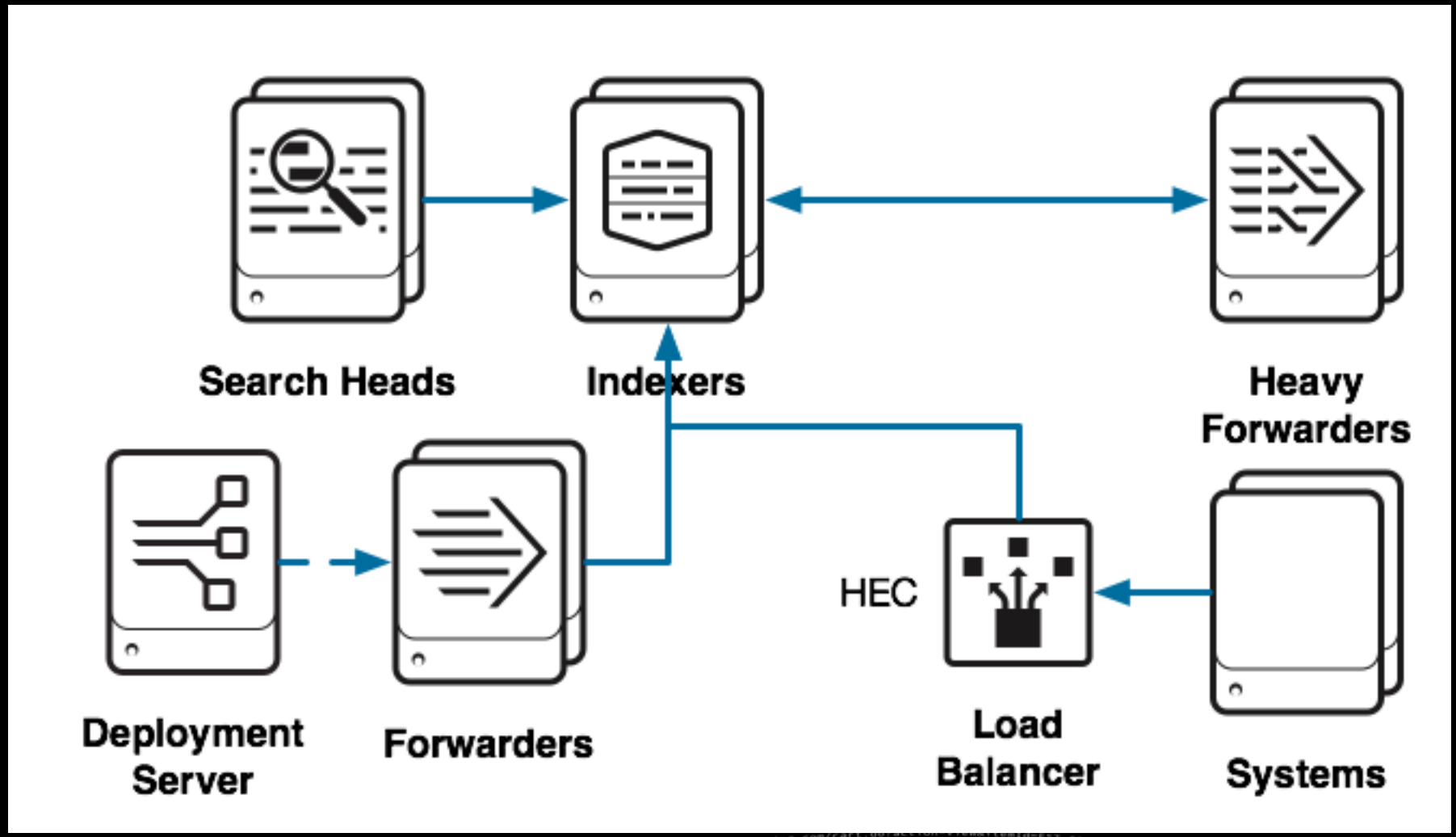
splunk> .conf18

Our Splunk Architecture

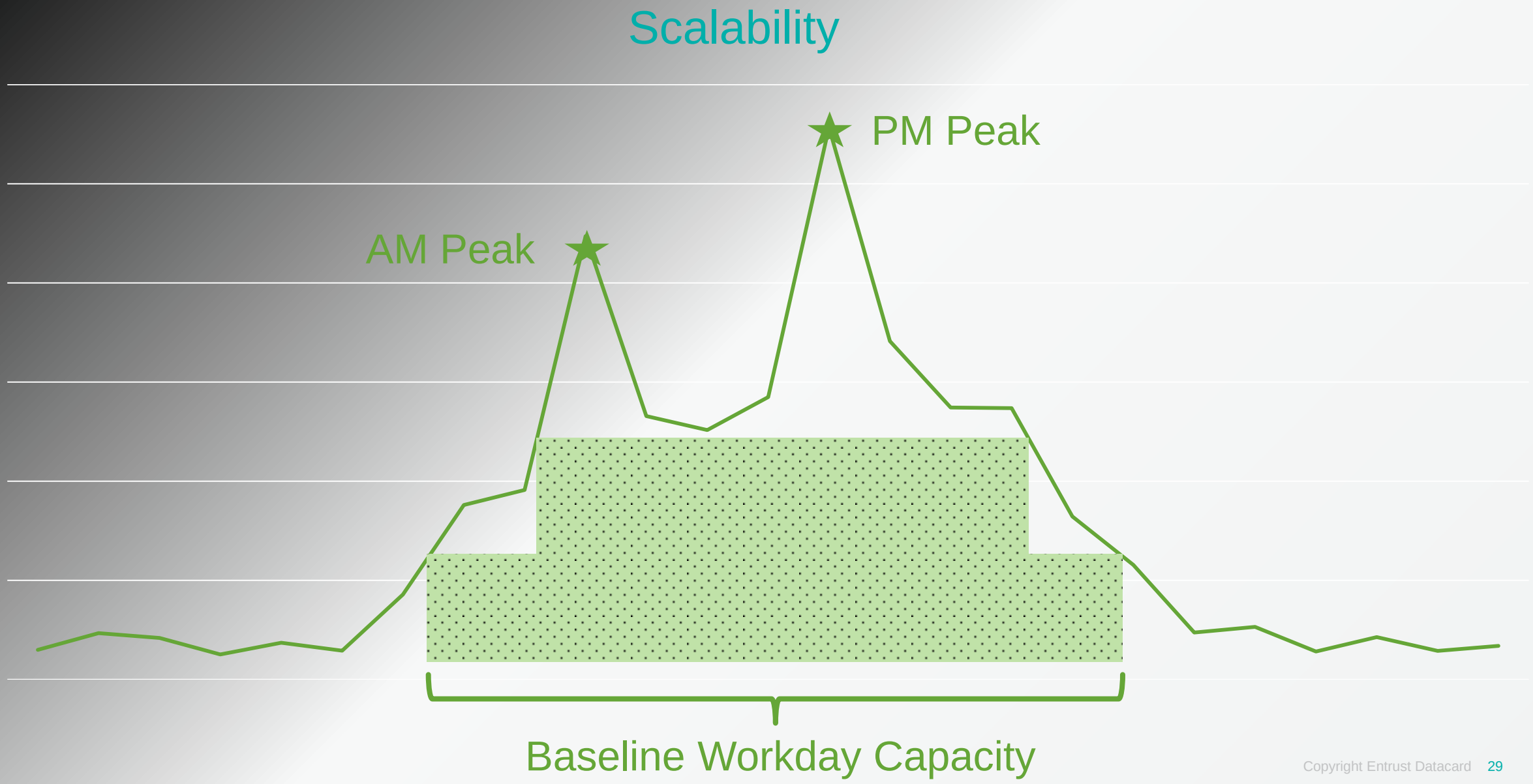


Architecture Deep Dive

View of a Single Region



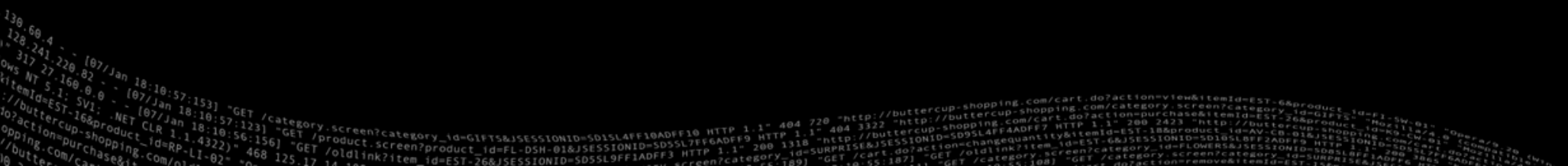
Not actual data. For illustration purposes only.



Splunk Scalability

How does it handle increases in log volume?

- Splunk can horizontally scale by adding more indexers
  - However, being a persistent workload, you can't easily scale down by removing indexers (like Casandra and other NoSQL DB's)
- Options for tackling scalability of log volumes
  - Over provisioning
  - Buffer logs during peaks (HEC, Kinesis, etc..)
  - Some combination of the two
- We decided on over provisioning to avoid data latency
- Alert on buffering



Key Takeaways

Using Splunk for Cloud Native Workloads

1. Use DevOps approach for implementing monitoring
   - Dev involvement
   - Automation
2. Iterative approach
   - Feedback loop from operational experience to design
3. Design monitoring into the application
   - Publish application metrics
   - Optimize log messages
4. Embrace the CIM and develop your own data models to simplify comparing related data
5. Monitor your monitoring tools
6. Leverage experts

Thank You

Don't forget to rate this session in the .conf18 mobile app