

splunk> .conf2017

Monitoring End User Experiences With Splunk and New Relic

Break down the silos in your observability infrastructure.

Abner Germanow | New Relic, Partner Marketing & Evangelism

Tom Martin | Splunk, Staff ITOA Practitioner

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.

New Relic At A Glance:

NEWR

NYSE – 2014

15k+

Customers

1.5B

Scale: Events & Metrics Per Minute

1,700+ Global Enterprises

13,500+ Disruptors



Adobe

News Corp



CONDÉ NAST

HealthCare.gov



GROUPON



NORDSTROM rack



DOW JONES



trainline



HAUTELOOK
— A NORDSTROM COMPANY —



intuit



Confused.com



Hotel Tonight

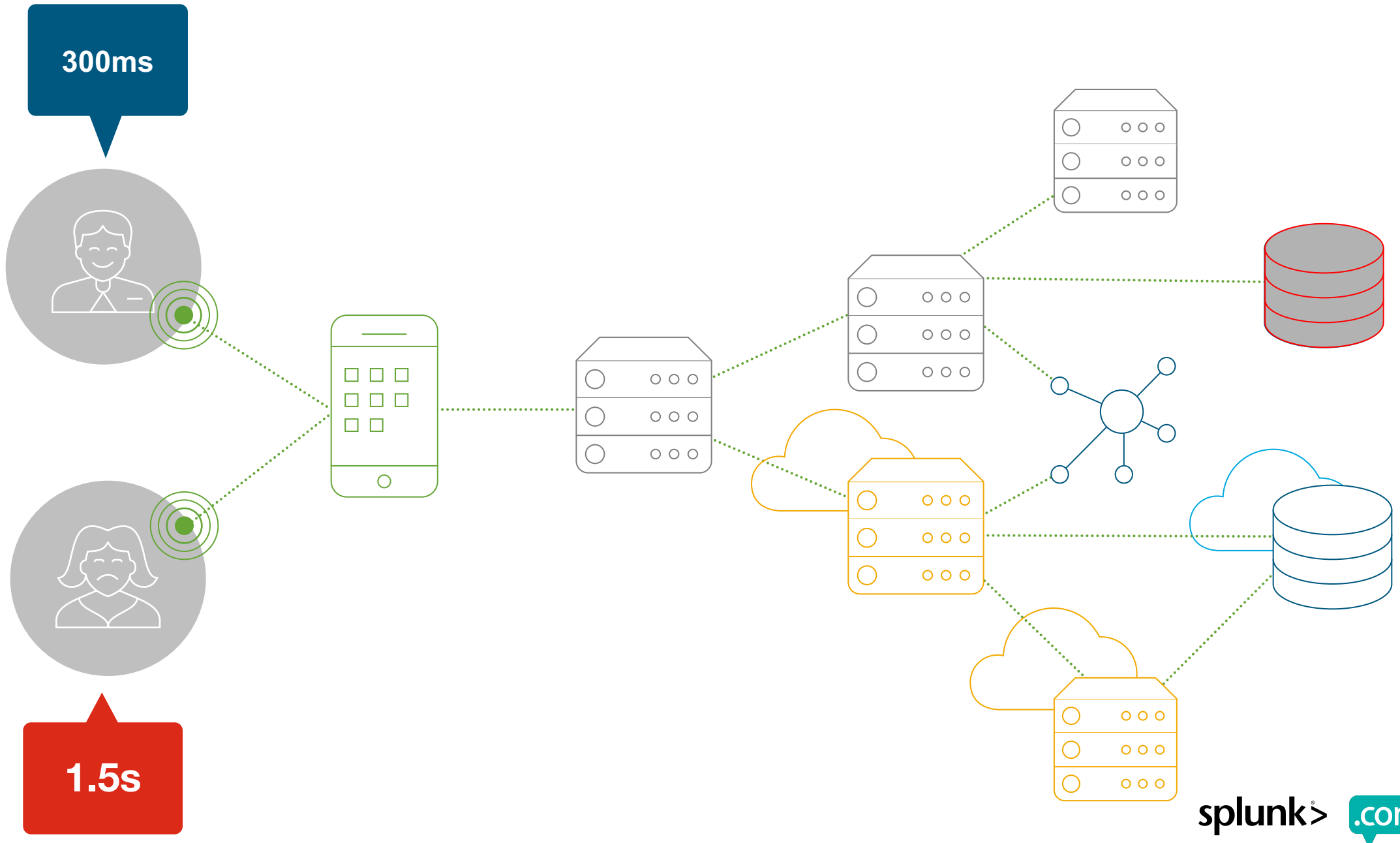
splunk

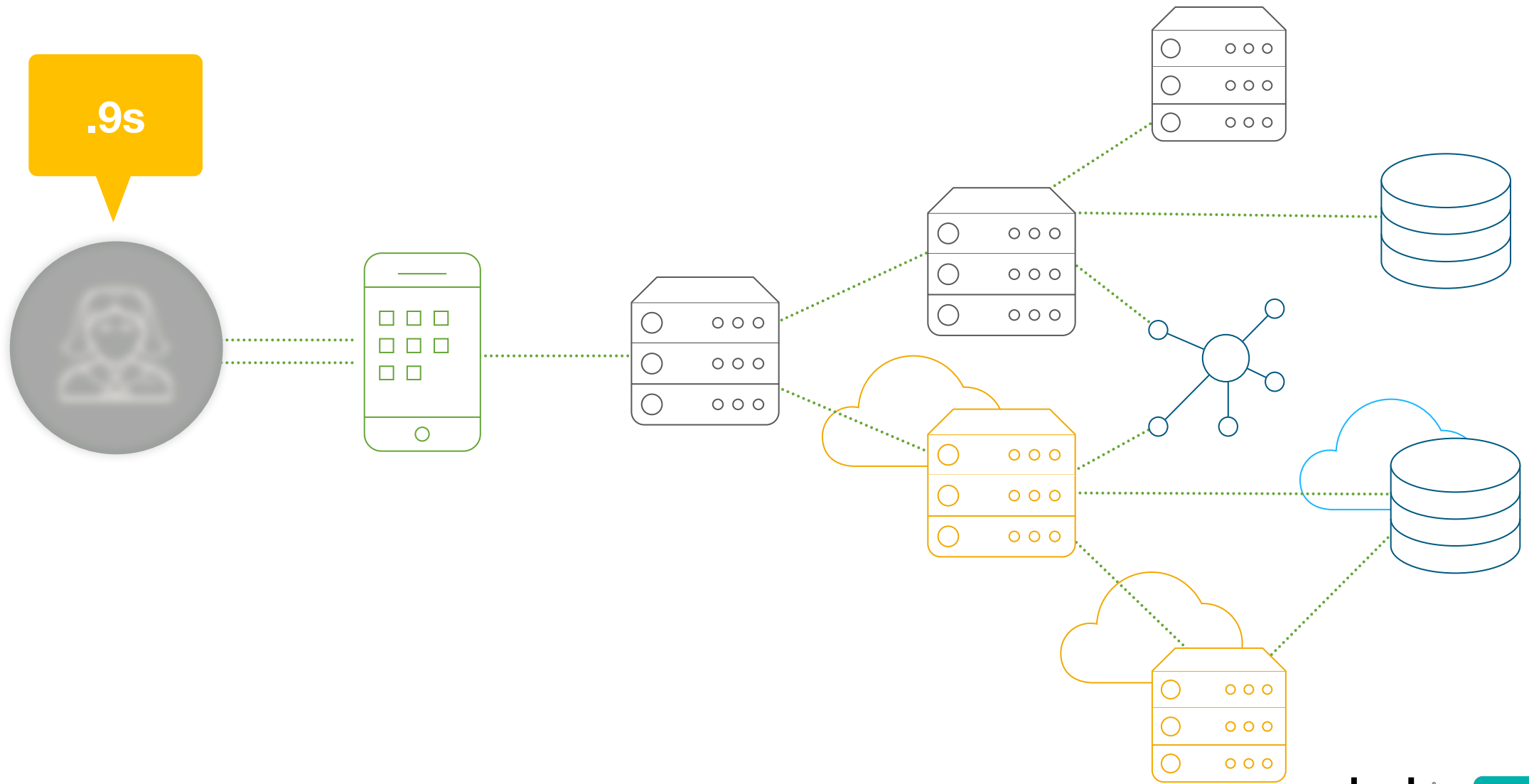


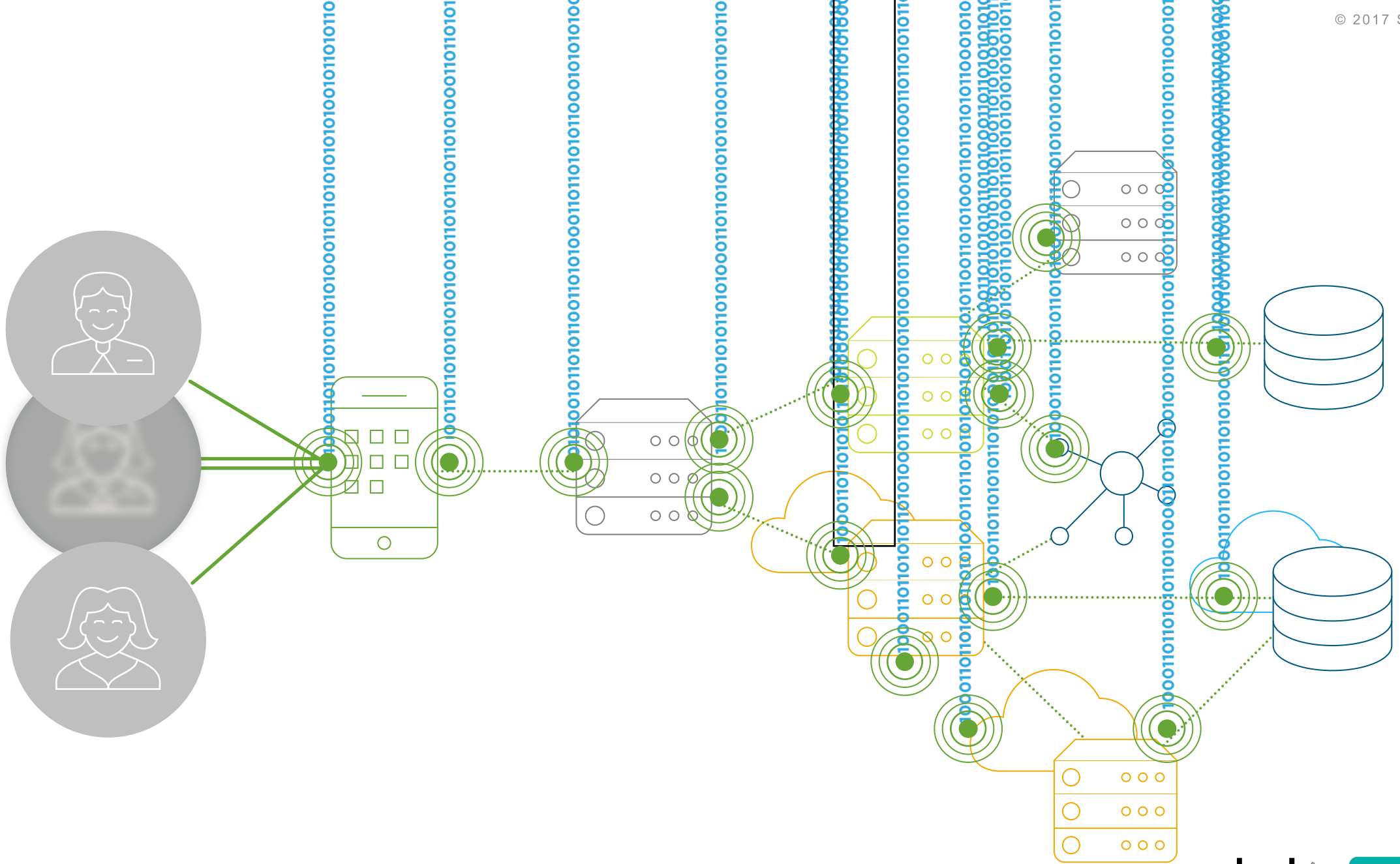
© 2008-17 New Relic, Inc. All rights reserved. New Relic.

splunk>

Confidential. ©2008–17 New Relic, Inc. All rights reserved







Lots of Data Sources



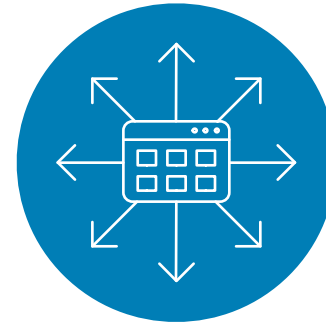
Mobile SDK



Browser Agents



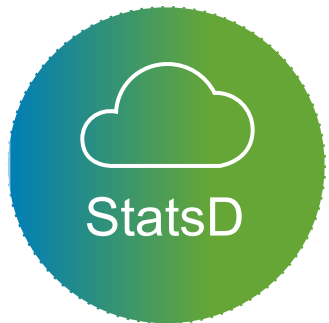
Synthetic Users



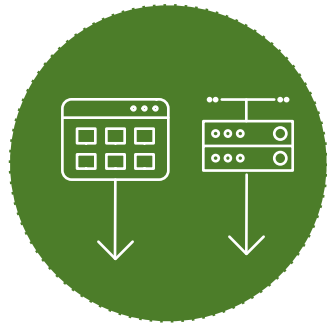
Application Agents



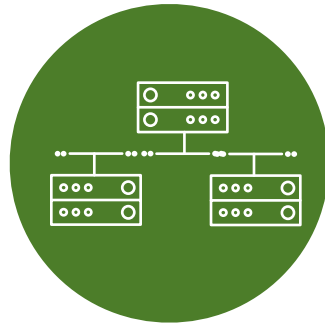
Infrastructure Agents



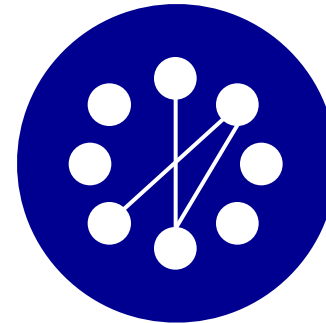
Cloud & Custom Metrics



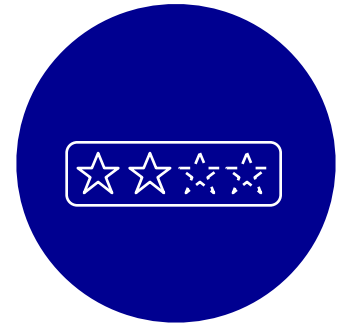
Logging / Machine Data



Wire Data



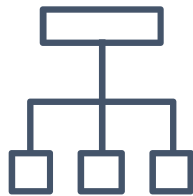
Synthetic Infrastructure



Social & Contact Center

From any source, monitoring data can be organized into three main categories

Traces



*Relationships
between events*

Examples

Application components involved during a request with an error

New Relic Provides



Metrics



*Measurement
of an event*

Throughput, error rate, request rate, request duration



Logs



*Human-readable
events*

System startup output, process output

**via Splunk Integrations*



splunk>

.conf2017

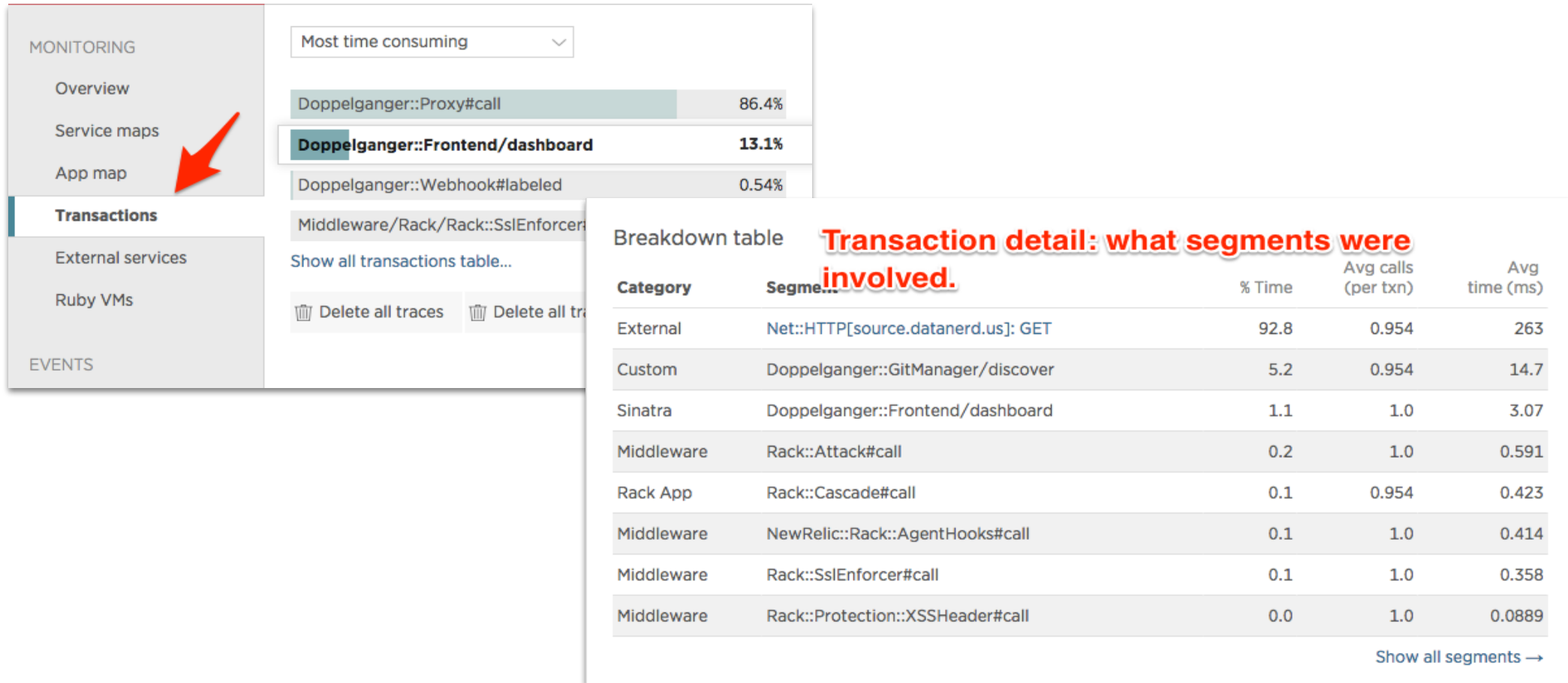
splunk **.conf2017**

CONFIDENTIAL ©2008–17 New Relic, Inc. All rights reserved.

 New Relic.

A line drawing of a woman with her hair in a bun, wearing glasses and a collared shirt, looking down at a laptop. The laptop screen is blank.

Transactions Are a Central Part of New Relic's Product and Help Developers Diagnose and Troubleshoot Many Problems Without Guessing.



MONITORING

- Overview
- Service maps
- App map
- Transactions**
- External services
- Ruby VMs

EVENTS

Most time consuming

Transaction	Percentage
Doppelganger::Proxy#call	86.4%
Doppelganger::Frontend/dashboard	13.1%
Doppelganger::Webhook#labeled	0.54%

Show all transactions table...

Delete all traces Delete all traces

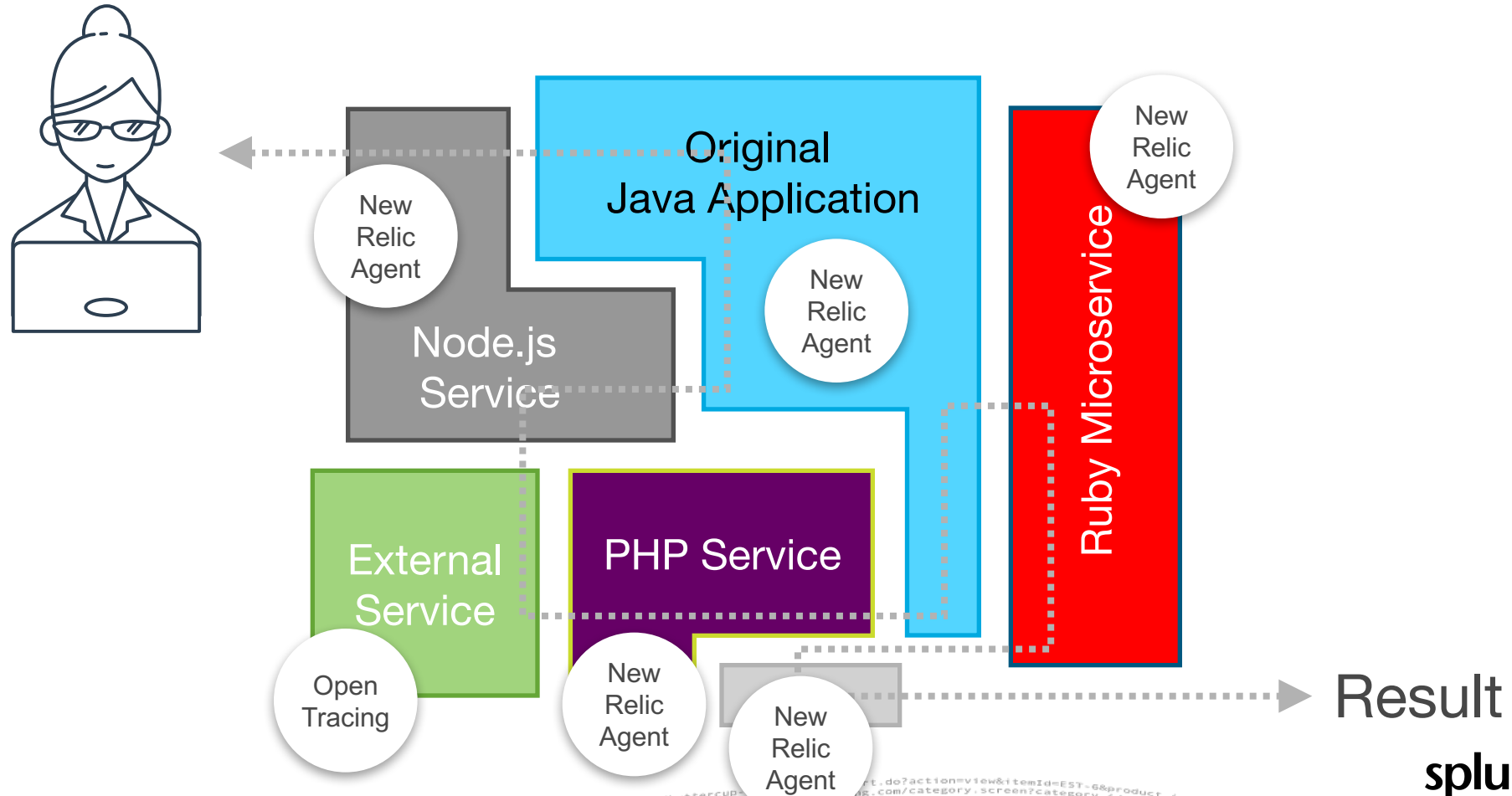
Breakdown table

Transaction detail: what segments were involved.

Category	Segment	% Time	Avg calls (per txn)	Avg time (ms)
External	Net::HTTP[source.datanerd.us]: GET	92.8	0.954	263
Custom	Doppelganger::GitManager/discover	5.2	0.954	14.7
Sinatra	Doppelganger::Frontend/dashboard	1.1	1.0	3.07
Middleware	Rack::Attack#call	0.2	1.0	0.591
Rack App	Rack::Cascade#call	0.1	0.954	0.423
Middleware	NewRelic::Rack::AgentHooks#call	0.1	1.0	0.414
Middleware	Rack::SslEnforcer#call	0.1	1.0	0.358
Middleware	Rack::Protection::XSSHeader#call	0.0	1.0	0.0889

Show all segments →

With Microservices, Applications ("Monoliths") Get Broken Up Into Smaller Pieces. The Traces *Now Go Through Multiple Programs.*





What's The Problem New Relic & Splunk Are Trying To Solve?

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D5SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FI-SW-03"
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D5SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FI-SW-03"

2 cloud regions
3 deploys/day

splunk> .conf2017

©2008–17 New Relic, Inc. All rights reserved. New Relic

2 cloud regions
3 deploys/day

splunk> .conf2017

©2008–17 New Relic, Inc. All rights reserved. New Relic



2 cloud regions
3 deploys/day

splunk> .conf2017

©2008–17 New Relic, Inc. All rights reserved. New Relic

2 cloud regions
3 deploys/day

splunk> .conf2017

©2008–17 New Relic, Inc. All rights reserved. New Relic



2 cloud regions
3 deploys/day

splunk> .conf2017

©2008–17 New Relic, Inc. All rights reserved. New Relic

Each tool, framework, platform and language has unique operational questions.



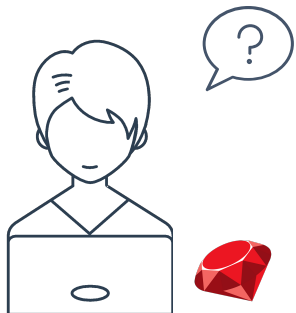
What's the error rate of my Java application?

Java Engineer



What's our spend in us-west-2?

VP of IT Infrastructure



Is the database slowing down Rails?

Web Developer

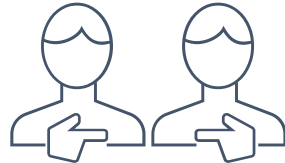


How can we improve deploys to Amazon ECS?

Site Reliability Engineer

Important operational data becomes siloed by service, app, or infrastructure type.

Operations



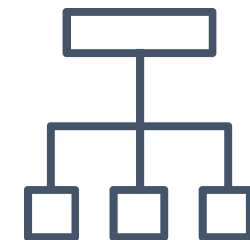
Infrastructure Metrics

Backend



Java application logs

Frontend



Application logs

splunk> .conf2017

New Relic

130.60.4 - - [07/Jan 18:10:57:153]
128.241.220.82 - - [07/Jan 18:10:57:153]
ows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14 - - [07/Jan 18:10:57:153]
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14 - - [07/Jan 18:10:57:153]
ofaction=purchase-shopping.com/ol
ofaction=purchase-shopping.com/ol
ofaction=purchase-shopping.com/ol

©2008-17 New Relic, Inc. All rights reserved

New Relic consolidates operational data to answer hard questions *across* teams, apps, and platforms.

Operations



Backend



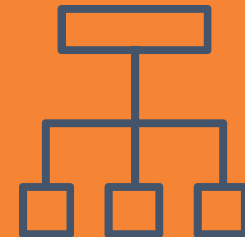
Frontend



Infrastructure Metrics

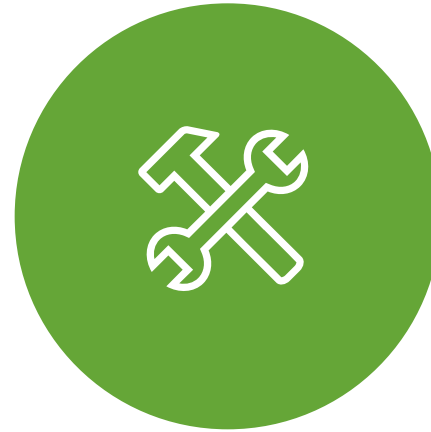


Java application logs



Application Traces

Why would you want this?



Reduce MTTR with
production log insights

+

metric-based application
monitoring

See real-time application
behaviors with byte-code
instrumentation data
in Splunk

See Splunk infra &
security alerts
in New Relic

Data Sources - Splunk and New Relic

Splunk Strengths

- ▶ Machine Data (specifically, around logs)
- ▶ Breadth across infrastructure (network, server, cloud infrastructure)
- ▶ Root cause analysis (often via config changes that are logged)
- ▶ Business-level KPIs, SLOs, etc. that span multiple applications
- ▶ Long term storage of raw management data

New Relic Strengths

- ▶ Dependencies across app (via Agents embedded inside apps & microservices)
- ▶ Breadth of Code level (BCI) (Java, .Net, Ruby, Node.js, PHP, Python, Go, iOS, Android, Javascript)
- ▶ End User Monitoring (response time, etc.)
- ▶ Real-time Trace/Transactions time-series data
- ▶ Ease of instrumentation & agent install

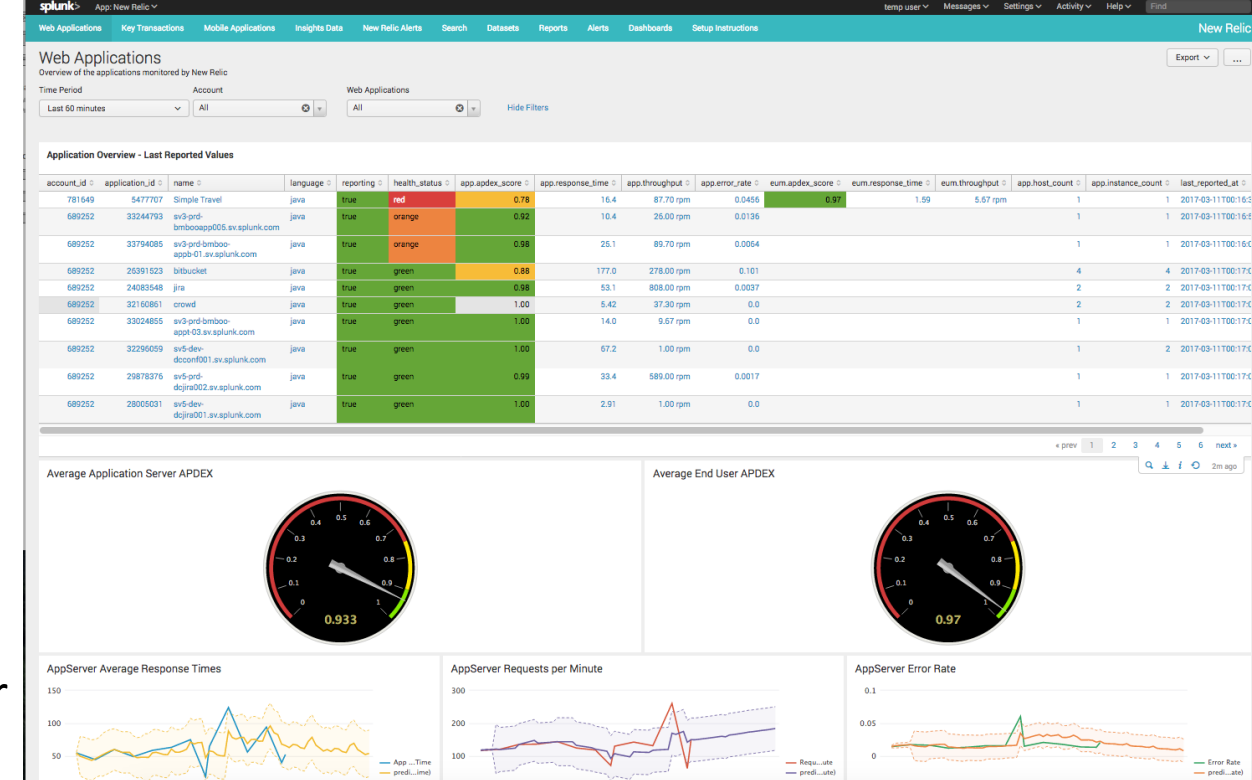


splunk  **.conf2017**

©2008–17 New Relic, Inc. All rights reserved.  New Relic.

Integration Highlights - Splunk App for New Relic

- ▶ Ease of integration with New Relic APIs to collect application, transaction, mobile, browser and synthetic performance and quality key performance indicators
- ▶ Out-of-the-box dashboards to summarize transaction response time, ApDex, errors and other key information
- ▶ Long term storage of data collected by New Relic add-on



The screenshot shows the 'Add New Relic Account Summary' form. The form has the following fields and options:

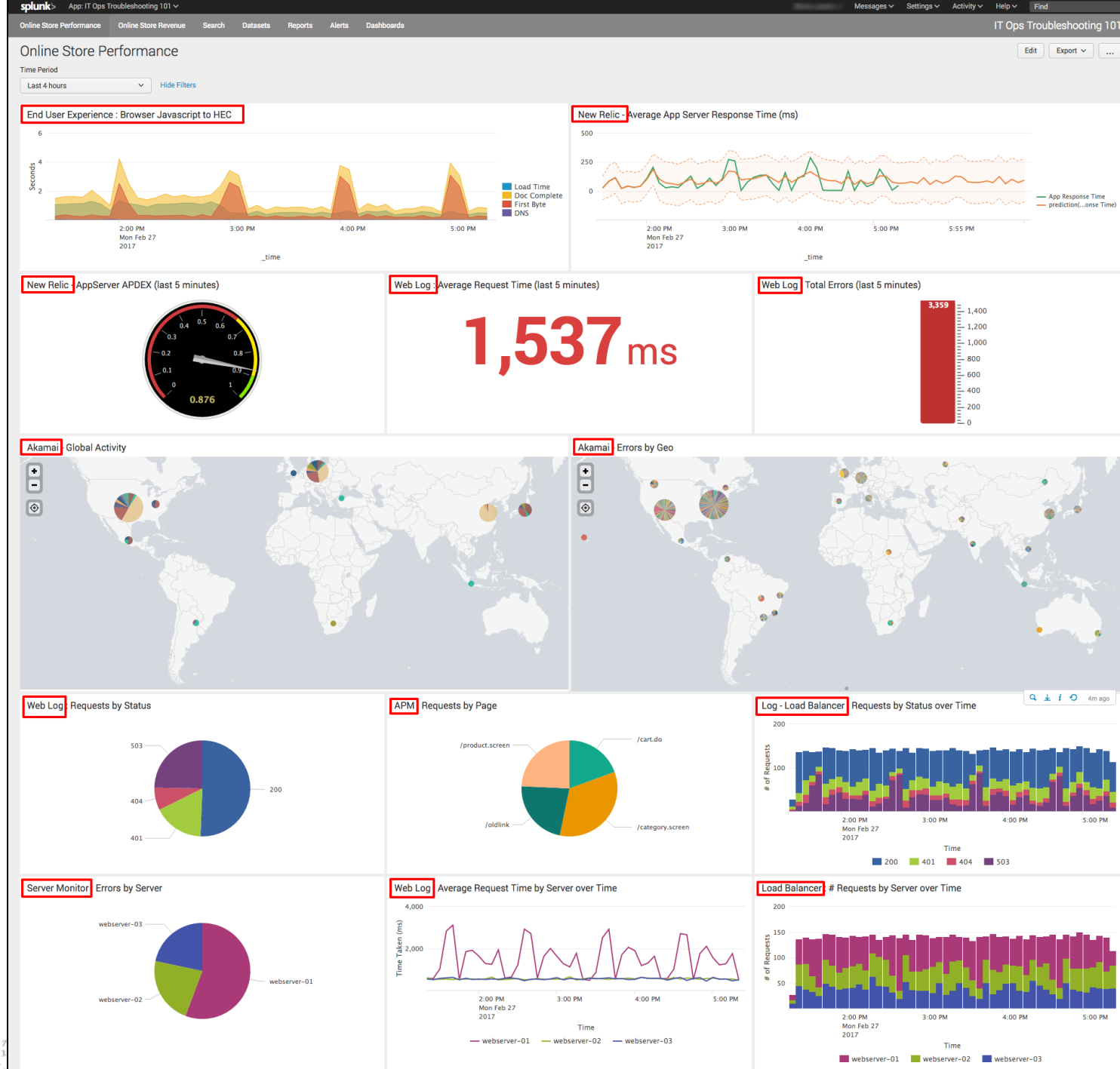
- Name ***: A text input field with a placeholder 'Enter a unique name for the data input'.
- Interval ***: A text input field with a placeholder 'Time interval of input in seconds'.
- Index ***: A dropdown menu with 'default' selected.
- New Relic Account Number ***: A text input field with a placeholder 'This can be found in the URL when you log into New Relic. e.g. https://rpm.newrelic.com/accounts/#####/...'.
- New Relic API Key ***: A text input field with a placeholder 'Your API Key can be found here: https://rpm.newrelic.com/accounts/#####/integrations?page=api_keys'.
- Metric Sets to Collect ***: A set of checkboxes for 'APM', 'Key Transactions', 'Mobile Applications', and 'Alert Violations'. All four are currently checked.

At the bottom of the form, there is a 'Cancel' button on the left and an 'Add' button on the right. Below the 'Metric Sets to Collect' section, there is a note: 'Select the APIs you would like to collect.'

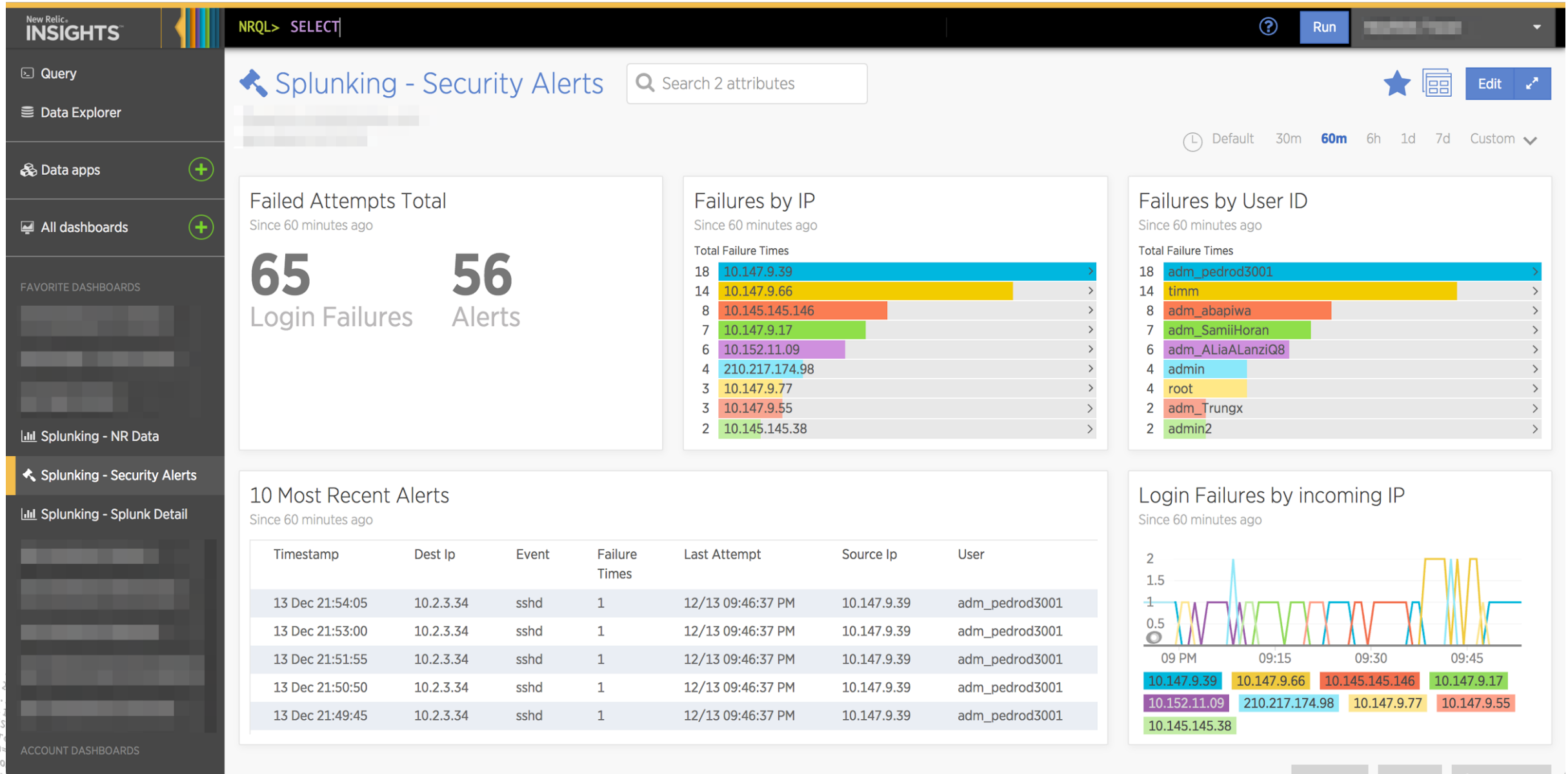


Splunk and New Relic: Break Down Silos

- ▶ Combine dashboard elements spanning many data sources
- ▶ Provide dashboards across many users
- ▶ Correlate time-series data based on Splunk Search Processing Language (SPL)



Splunk Alerts In New Relic



Integration Highlights - New Relic

- ▶ Splunk Reports in New Relic Insights to correlate code-level performance in New Relic, alongside detailed logs that provide additional context; for those using New Relic as their UI, having all the data in one place is valuable
- ▶ Ad-hoc querying of Splunk data to create flexible views of application logs against New Relic metrics and events for mobile, browser and APM
- ▶ Splunk Alerts available in context to APM and infrastructure monitoring via New Relic Insights
- ▶ In the long term, Splunk logs correlated to Transaction traces in APM to give the full context about application performance issues



Deck under NDA until 03/23/17

Integration Example - Media Company

Situation

- ▶ App Dev and newly created “Dev Ops” teams have been the primary “buyer” for New Relic
- ▶ Operations team has been the primary “buyer” for Splunk
- ▶ Both teams would get more value by seeing monitoring data across entire environment

Splunk + New Relic

- ▶ Allows Operations team to see End User Monitoring and app server metrics alongside infrastructure components they are measuring
- ▶ DevOps teams can ad-hoc query Splunk and get events from Splunk, offering better insight into how infrastructure impacts the apps they are responsible for



A green circle containing a white icon of a crossed wrench and hammer, symbolizing construction or maintenance.

Send Splunk Alerts to New Relic Insights

Thank You

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

splunk> .conf2017