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> .conf2017

New Relic At A Glance:

NEWR
NYSE – 2014

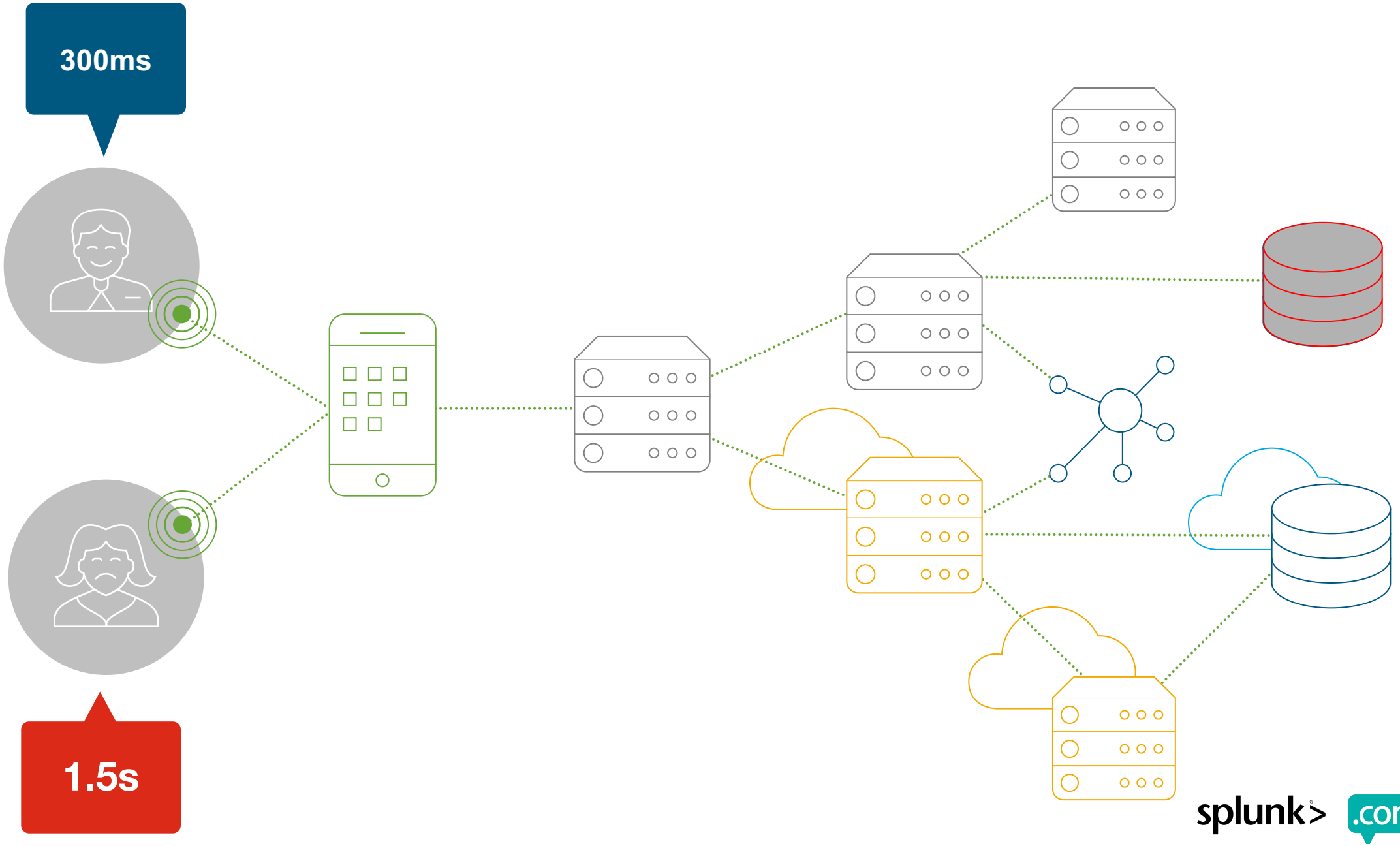
15k+
Customers

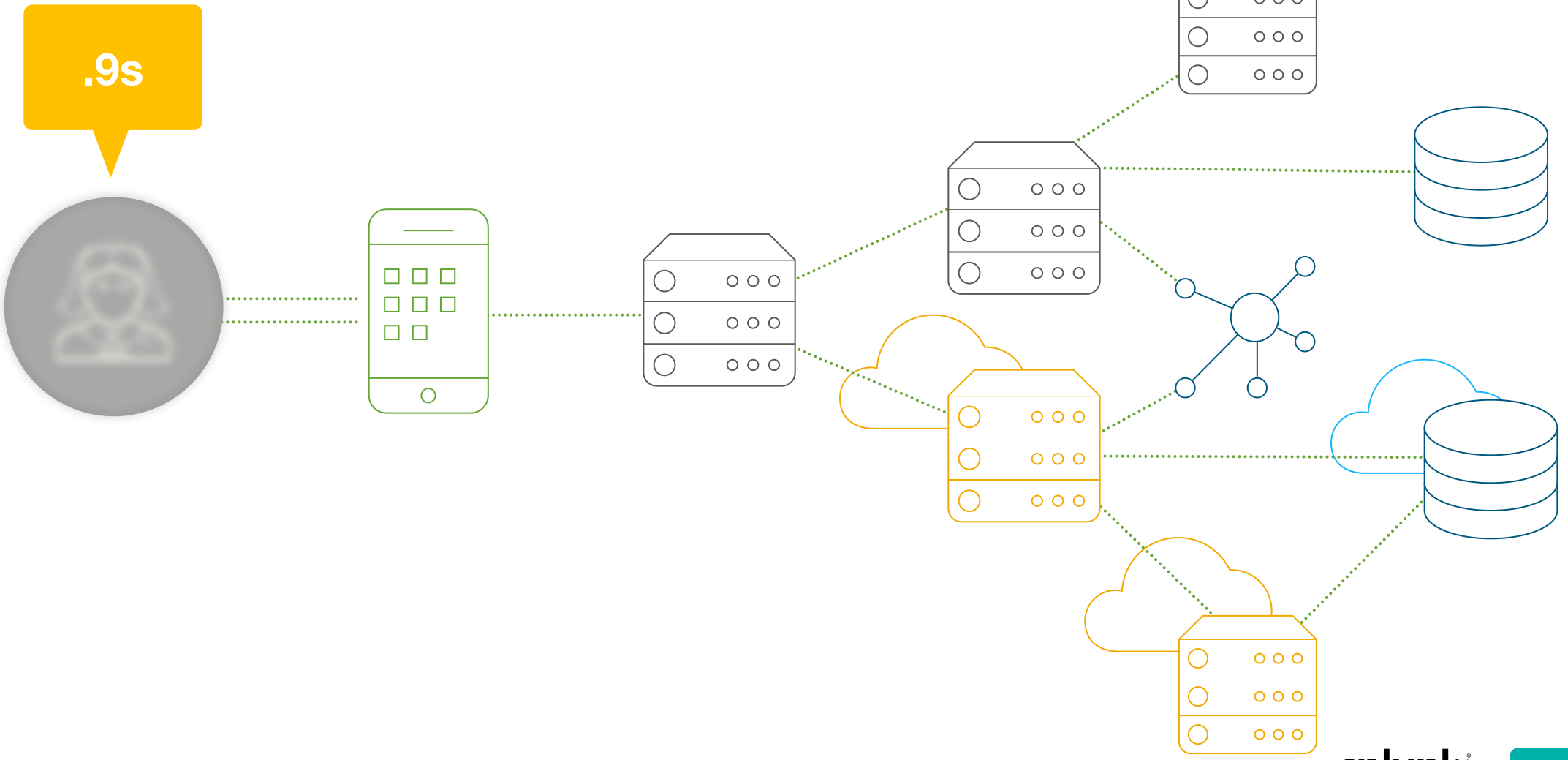
1.5B
Scale: Events & Metrics Per Minute

1,700+ Global Enterprises

13,500+ Disruptors

Why is monitoring hard?





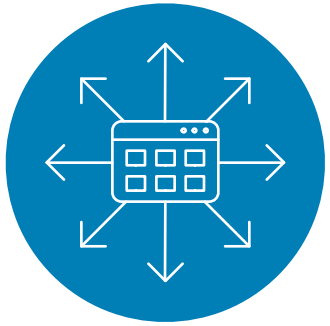
splunk> .conf2017

Lots of Data Sources

Mobile SDK

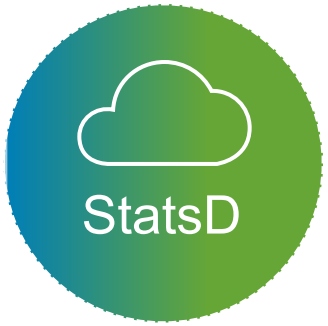
Browser Agents

Synthetic Users

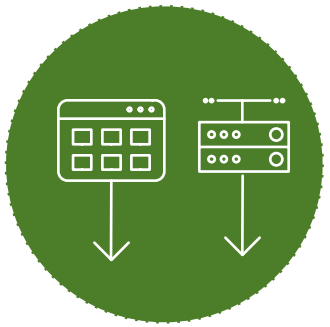


Application Agents

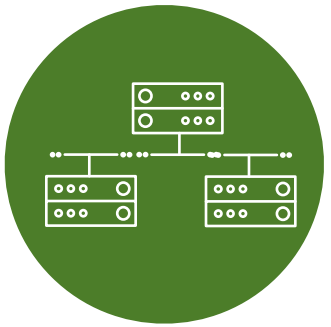
Infrastructure Agents



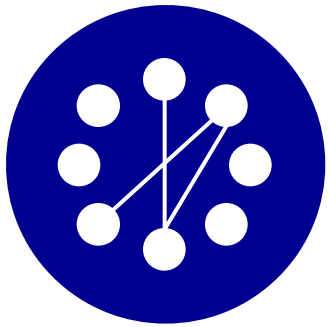
Cloud & Custom Metrics



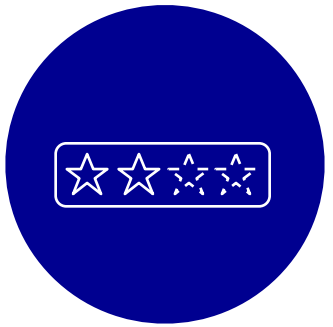
Logging / Machine Data



Wire Data



Synthetic Infrastructure



Social & Contact Center

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

		Examples	New Relic Provides
Traces	*Relationships between events*	Application components involved during a request with an error	✓
Metrics	*Measurement of an event*	Throughput, error rate, request rate, request duration	✓
Logs	*Human-readable events*	System startup output, process output	**via Splunk Integrations* ✓

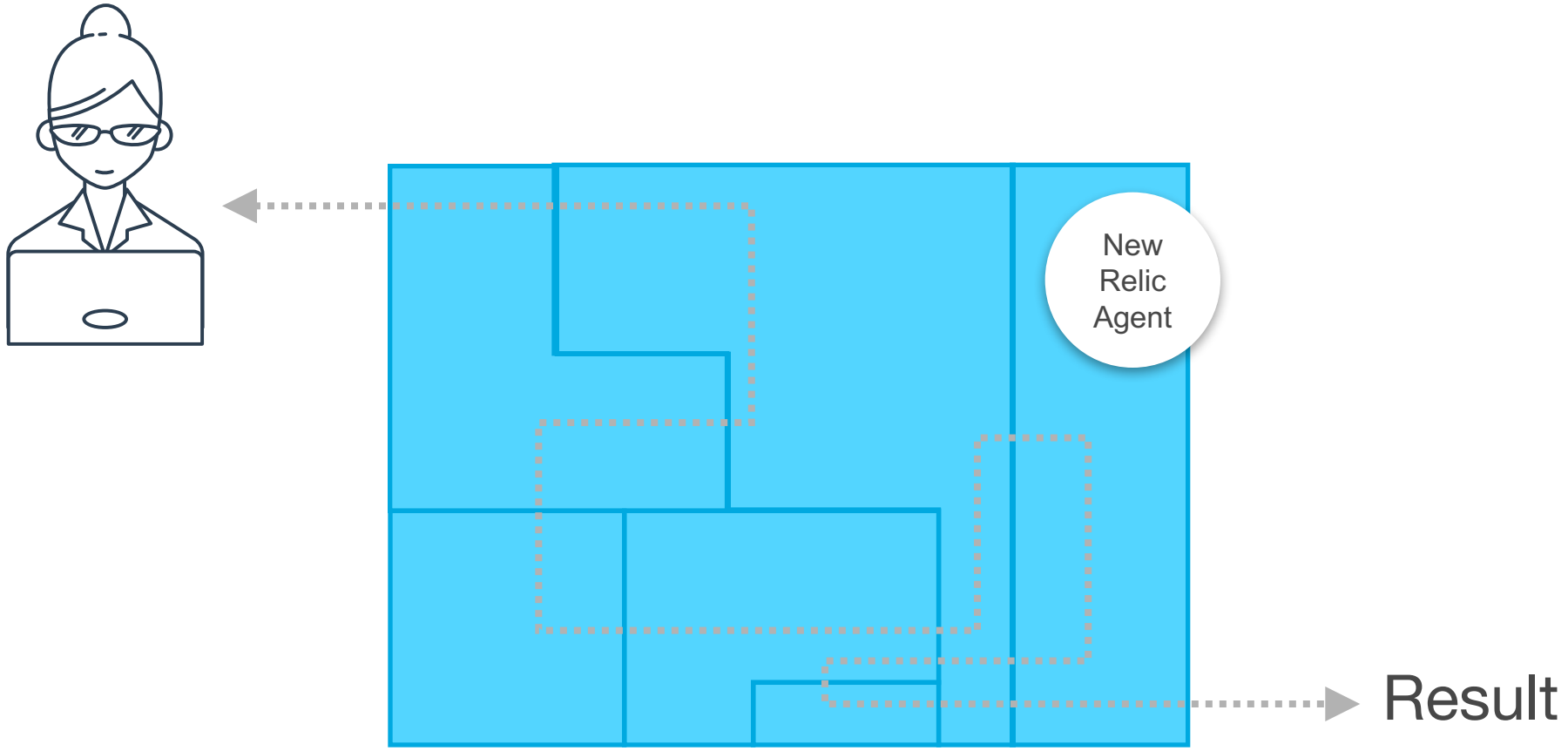
What is a transaction trace?

Traces: How Did an Application Arrive at a Result?

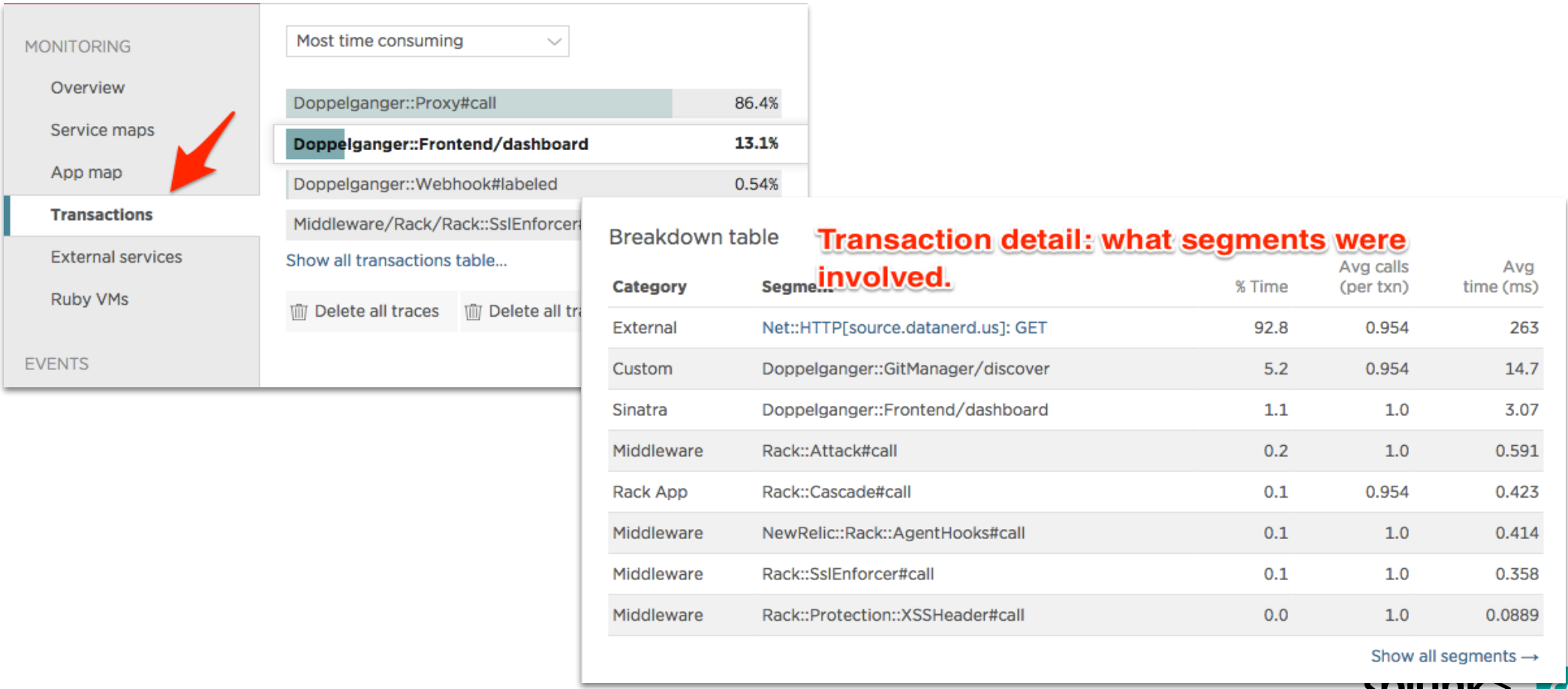
The Application

Result

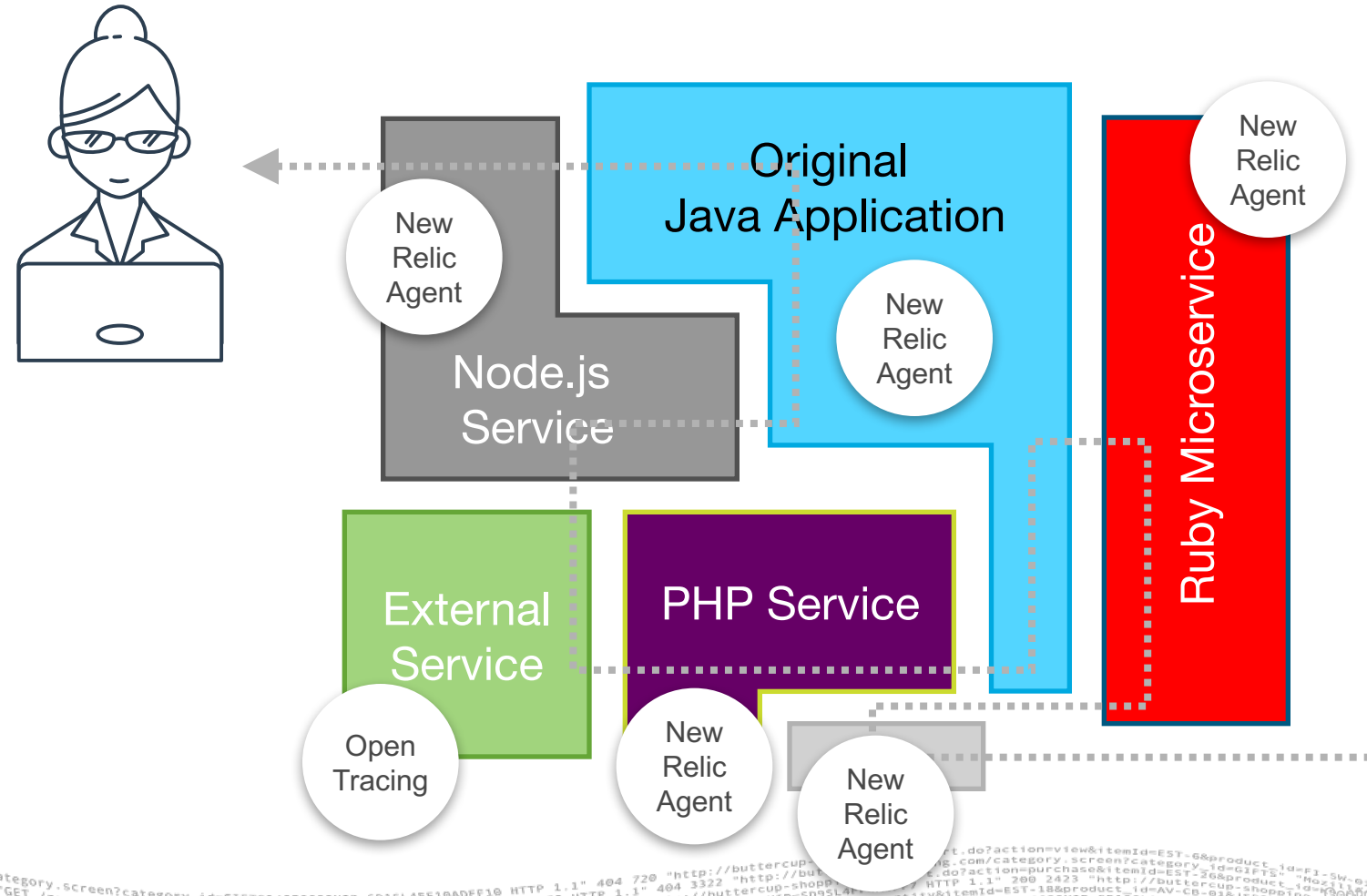
Tracing Provides Information on Which Segments of an Application Were Involved in a Result



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



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



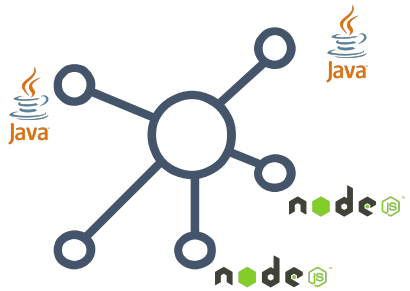
What's The Problem New Relic & Splunk Are Trying To Solve?

Volume of operational data being generated is growing exponentially.

Web App: *Then*

1 application
3 large servers
1 database
1 data center
1 deploy/quarter

Web App: Now



30 containers
4 services
10 small instances
2 managed services
2 databases
2 cloud regions
3 deploys/day

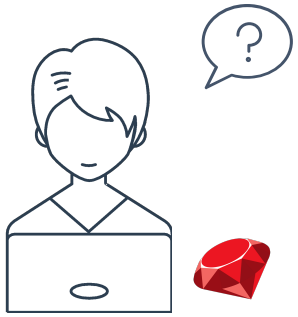
Each tool, framework, platform and language has unique operational questions.

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?

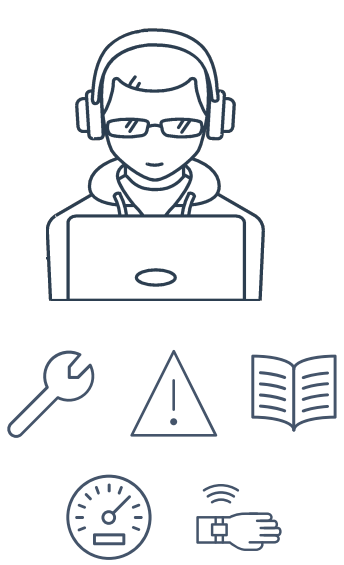
Web Developer

How can we improve deploys to Amazon ECS?

Site Reliability Engineer

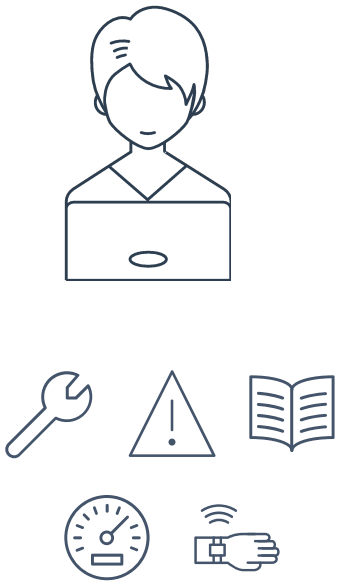
To answer operational questions, teams define their own metrics, logging, and alerting practices.

Operations



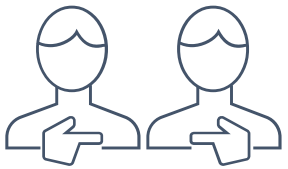
Backend

Frontend



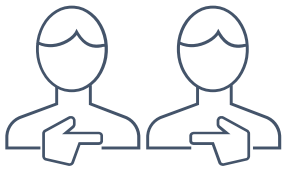
Important operational data becomes siloed by service, app, or infrastructure type.

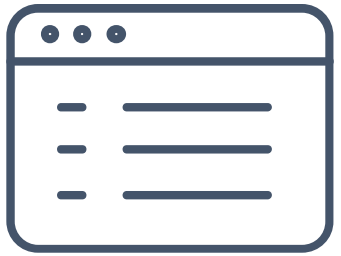
Operations



Infrastructure Metrics

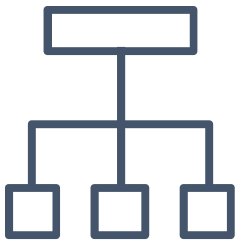
Backend





Java application logs

Frontend



Application traces

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

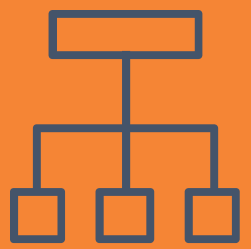
Operations

Infrastructure Metrics

Backend

Java application logs

Frontend



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

splunk> .conf2017

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

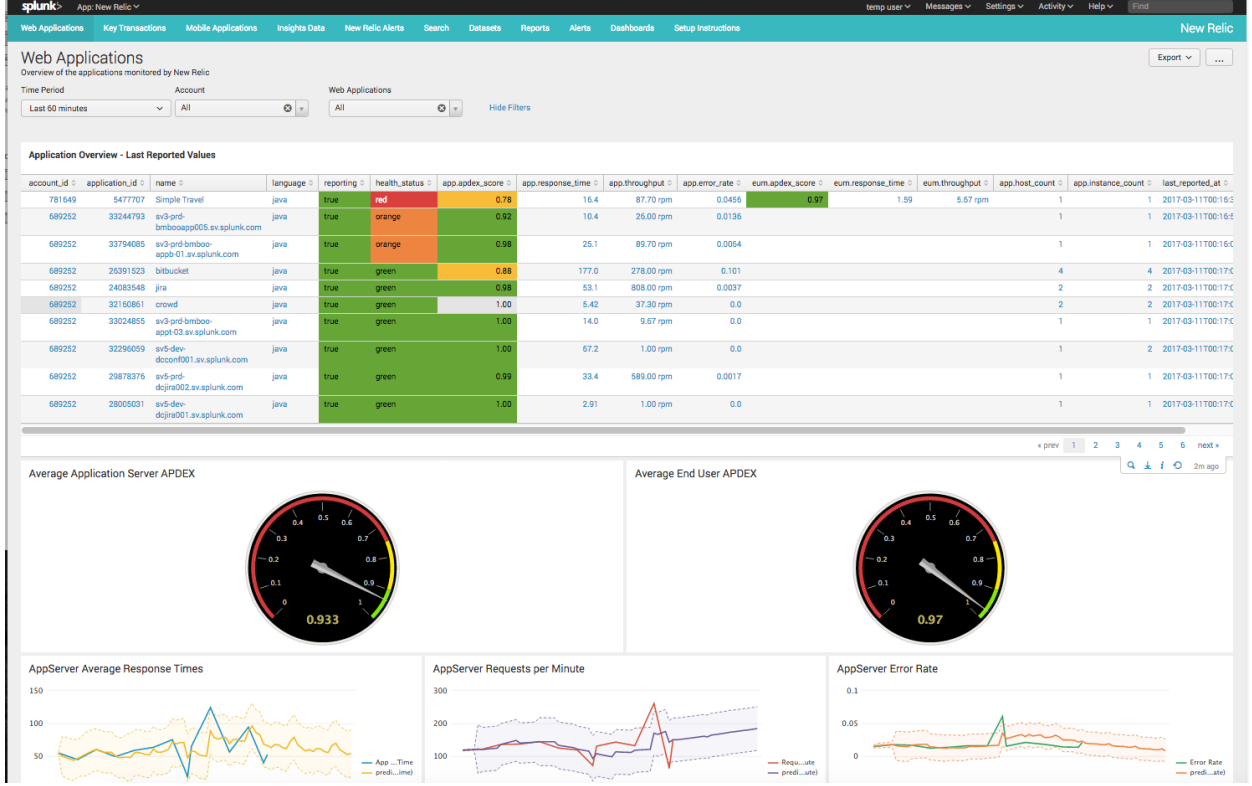
New Relic Strengths

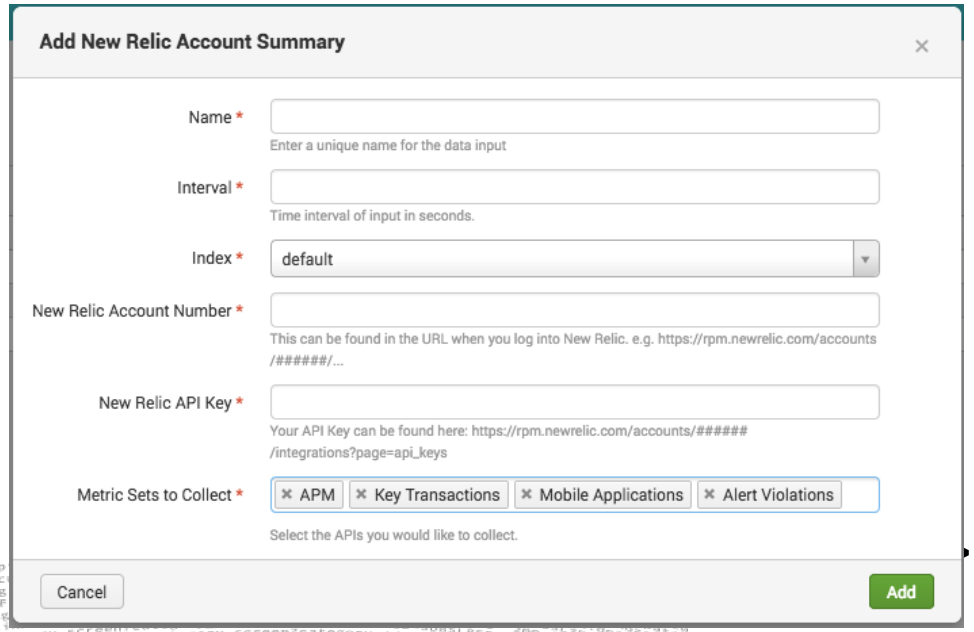
- Dependencies across app (via Agents embedded inside apps & microservices)
- Breadth of Code level (BCI) (Java, .Net, Ruby, Node.js, PHP, Python, Go, iOS, Android, Javascript)
- End User Monitoring (response time, etc.)
- Real-time Trace/Transactions time-series data
- Ease of instrumentation & agent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

How about you demo this thing already?

Integration Highlights - Splunk App for New Relic

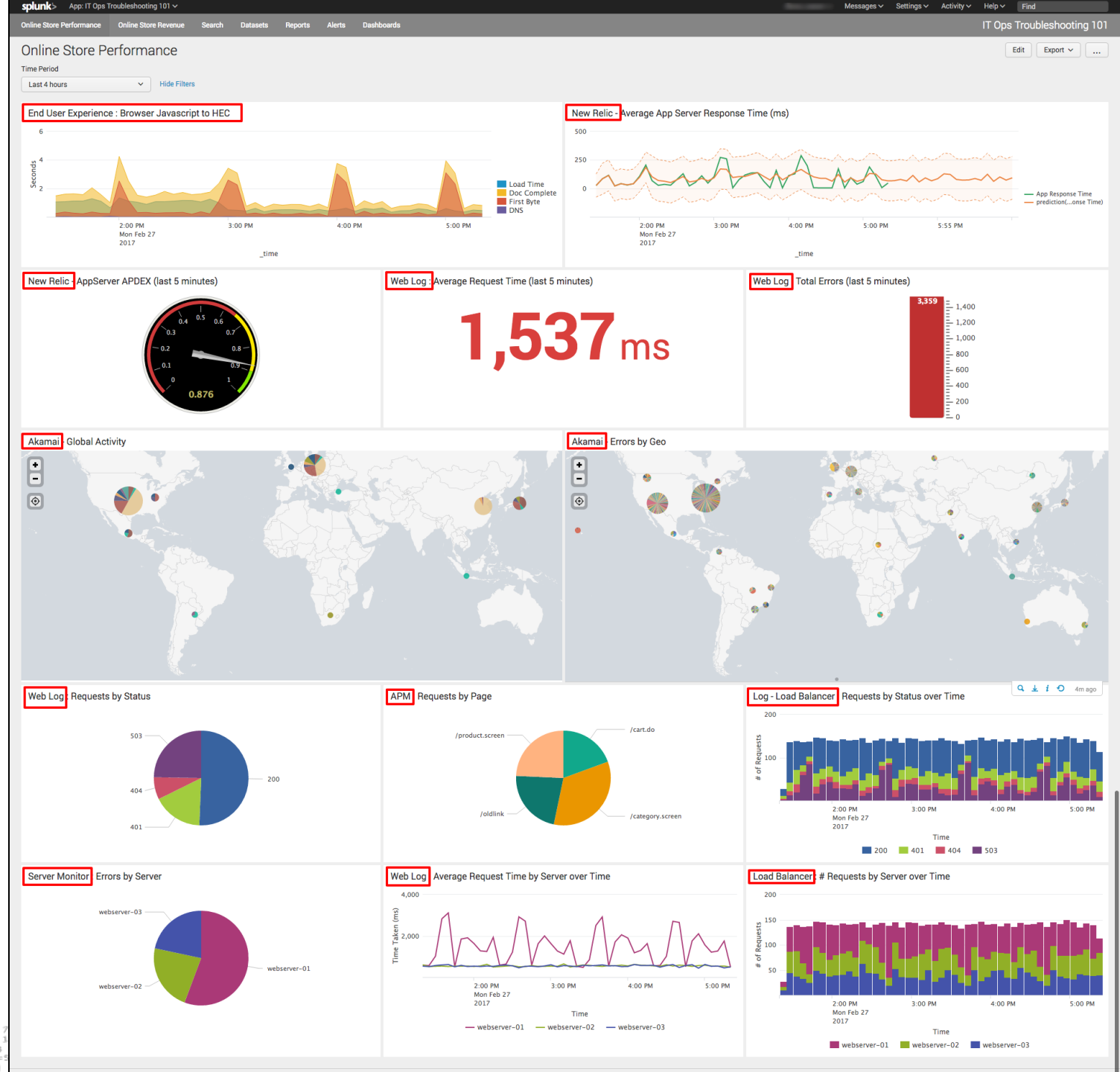
- Ease of integration with New Relic APIs to collect application, transaction, mobile, browser and synthetic performance and quality key performance indicators
- Out-of-the-box dashboards to summarize transaction response time, ApDex, errors and other key information
- Long term storage of data collected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



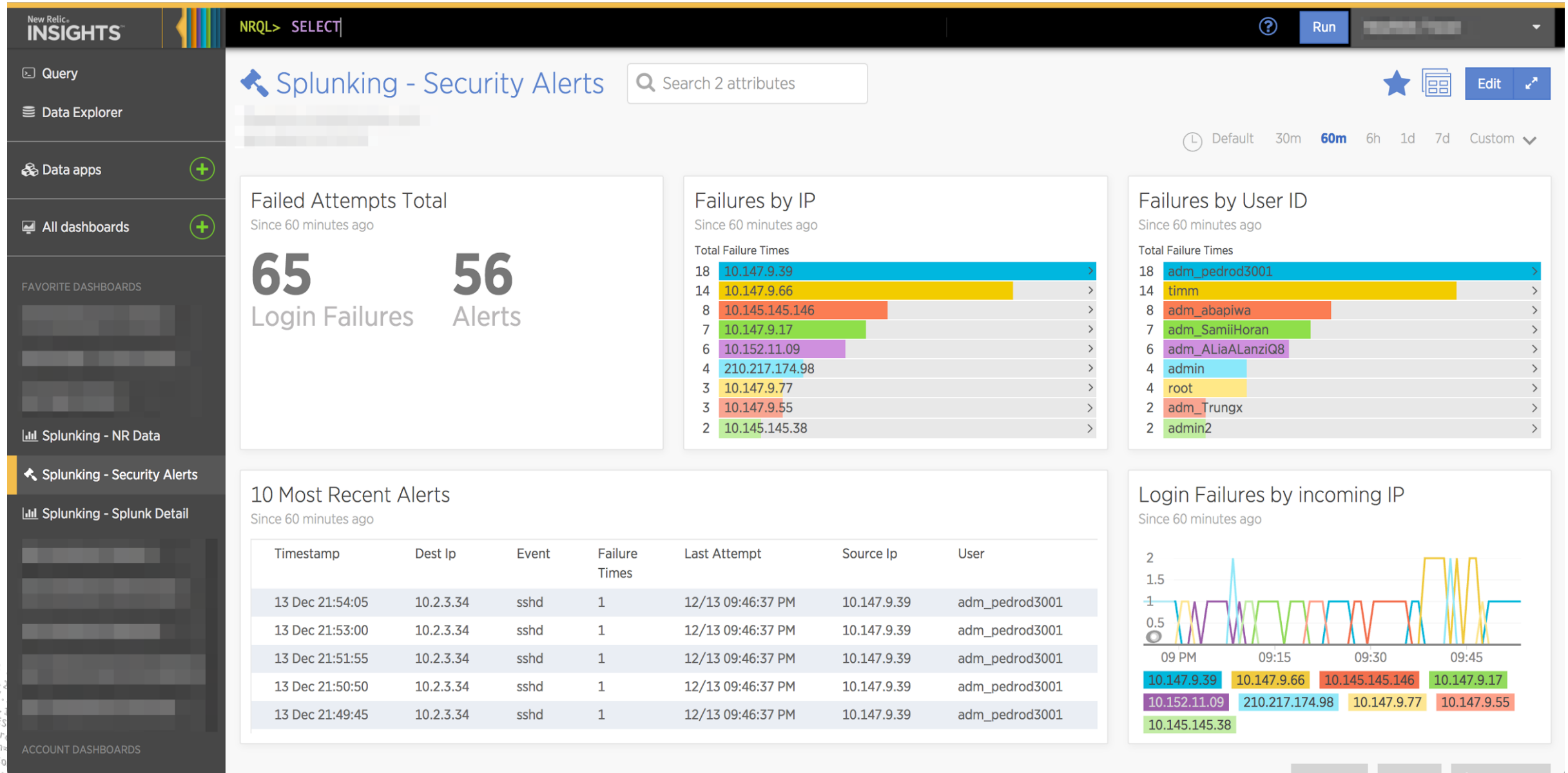


Splunk and New Relic: Break Down Silos

- 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

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

Deck under NDA until 03/23/17

What should you do next?

Have your New Relic license key?

Install the[Splunkbase plug-in](#)

Send Splunk Alerts to New Relic Insights

See pre-built dashboards in Splunk.

splunk> .conf2017

Thank You

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