Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

splunk> .conf21

Monitoring Your Valuable Data in Splunk at Scale With TrackMe, The Easy Way!

TRU1548B

Guilhem Marchand

Partner Professional Services | Octamis

splunk> .conf21

Guilhem Marchand

Partner Professional Services | Octamis

splunk> .conf21

Agenda

TrackMe is a complete application providing key monitoring capabilities for your Splunk data sources

1) The fundamental and crucial key monitoring

   Discover why properly monitoring your data sources is fundamental for a successful and valuable Splunk deployment

2) TrackMe in a nutshell

   Main concepts of TrackMe

3) Going further with advanced features

   When simplicity meets efficiency, discover advanced features that provide the required agility for everyone

4) Getting the best from TrackMe

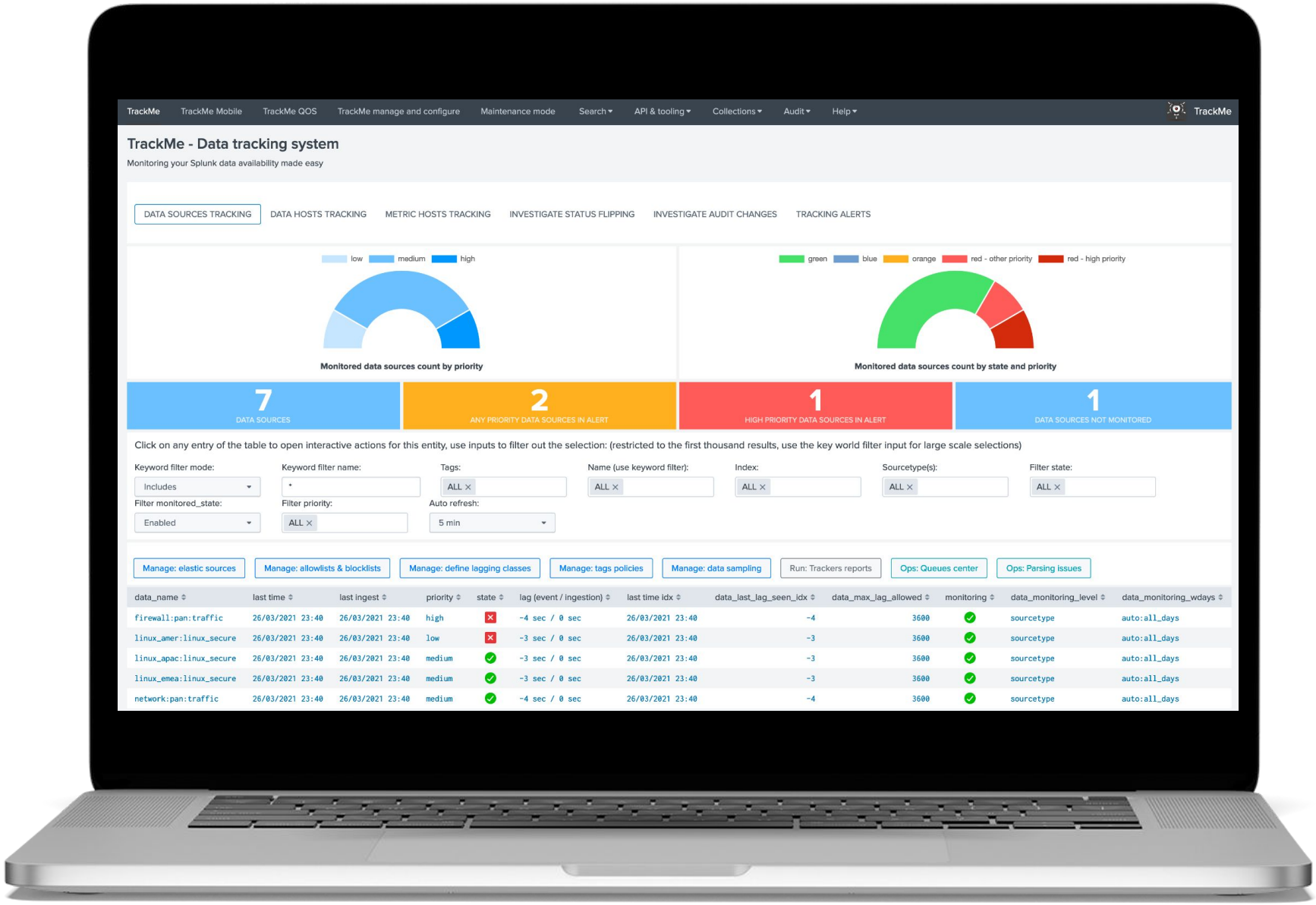
   Get successful in Production with third party interactions and integration such as Splunk ITSI

splunk> .conf21

TrackMe!

A single place to manage them all

This is where TrackMe stands, providing you with an **automated**, **easy** and **scalable** framework to discover and monitor your **valuable** data in Splunk!



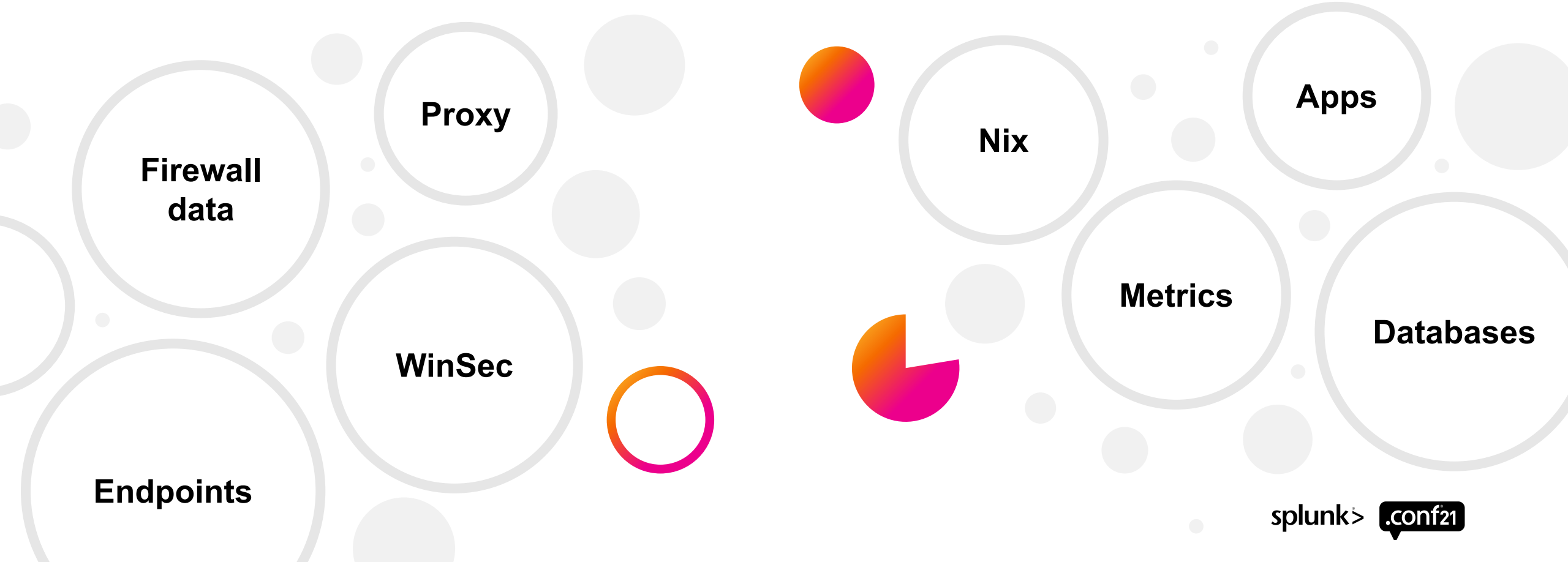
splunk> .conf21

Monitoring Your Data Sources is Fundamental

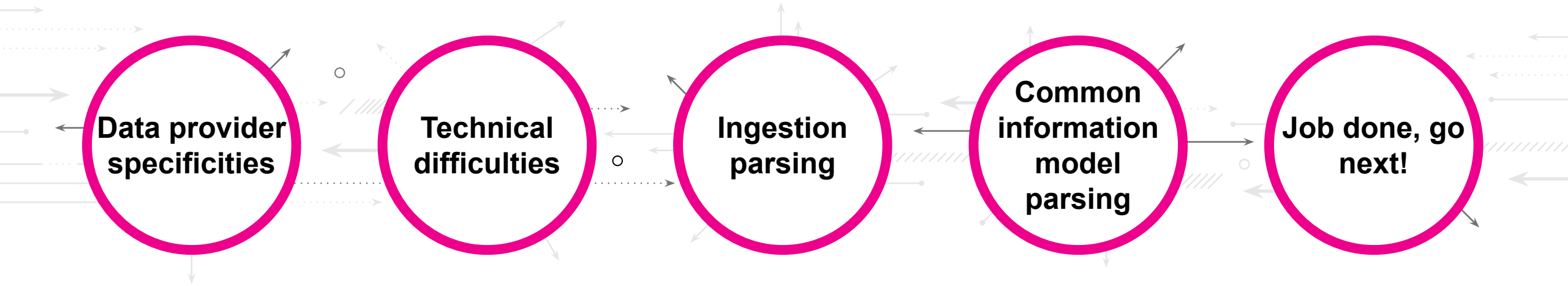
At the root of TrackMe stand crucial questions too often neglected

splunk> .conf21

With so many data sources, how to make sure things are still working as expected?



Data on-boarding is time consuming!
Once the data goes in, we too often neglect to monitor its availability and quality over time



Each data is a specific use case, some are well known and simple, some can be very tedious

There are always technical challenges we face and handle

When on-boarding data, quality matters

In a security context, CIM parsing is a key, this can be challenging

When big steps are done and data goes in, we often forget about it!

The fundamental activity of monitoring data sources' availability

Why would this be that critical?

- When data sources stop emitting data to Splunk, people administrating the deployment should **NEVER** be warned by the end users

- Most use cases are **USELESS** when the data is not present as expected, think about these amazing correlation searches your teams spent time, passion and money designing!

- Trust in the Splunk platform can be irremediability damaged, in some extreme cases missing critical data can **TOTALLY** annihilate the value of your $ investments in Splunk

TrackMe in a Nutshell

When easy concepts really mean BIG value

splunk> .conf21

How things work, in a few words!

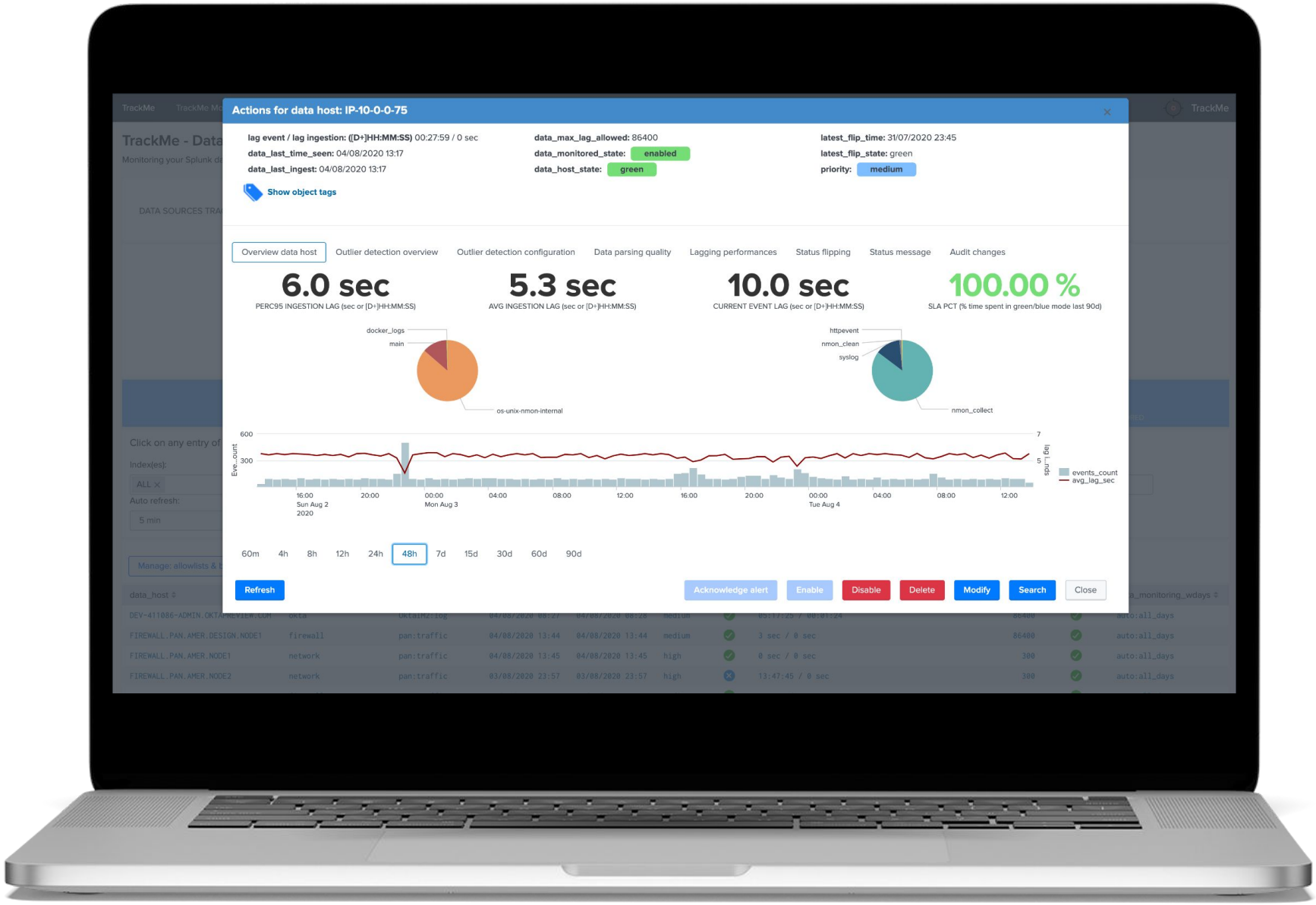
TrackMe tackles all the hard work for you

- TrackMe **discovers** and **maintains** every single data source in your environment automatically
- For **scaling** purposes, we use **tstats** based searches essentially
- Generic concepts are applied automatically, to handle **frequency** and expected **latency**
- **KPIs** are generated continuously (latency, delay, volume) and compared to the actual state
- Various rich features are available to handle **mass** and **granular** configuration items, from policies driving the monitoring rules to tagging and documenting your data sources
- **Quality** is inspected automatically too, with advanced features allowing to detect the bad things no one knows about, such as unexpected **parsing** failure at the ingestion

TrackMe Main UI

Easy user experience

TrackMe essentially consists in a single page **rich** user interface, allowing all user **interactions** easily



splunk> .conf21

Going Further with Advanced Features

Beyond the simple detection of delay and latency

splunk> .conf21

TrackMe is Rich in Features

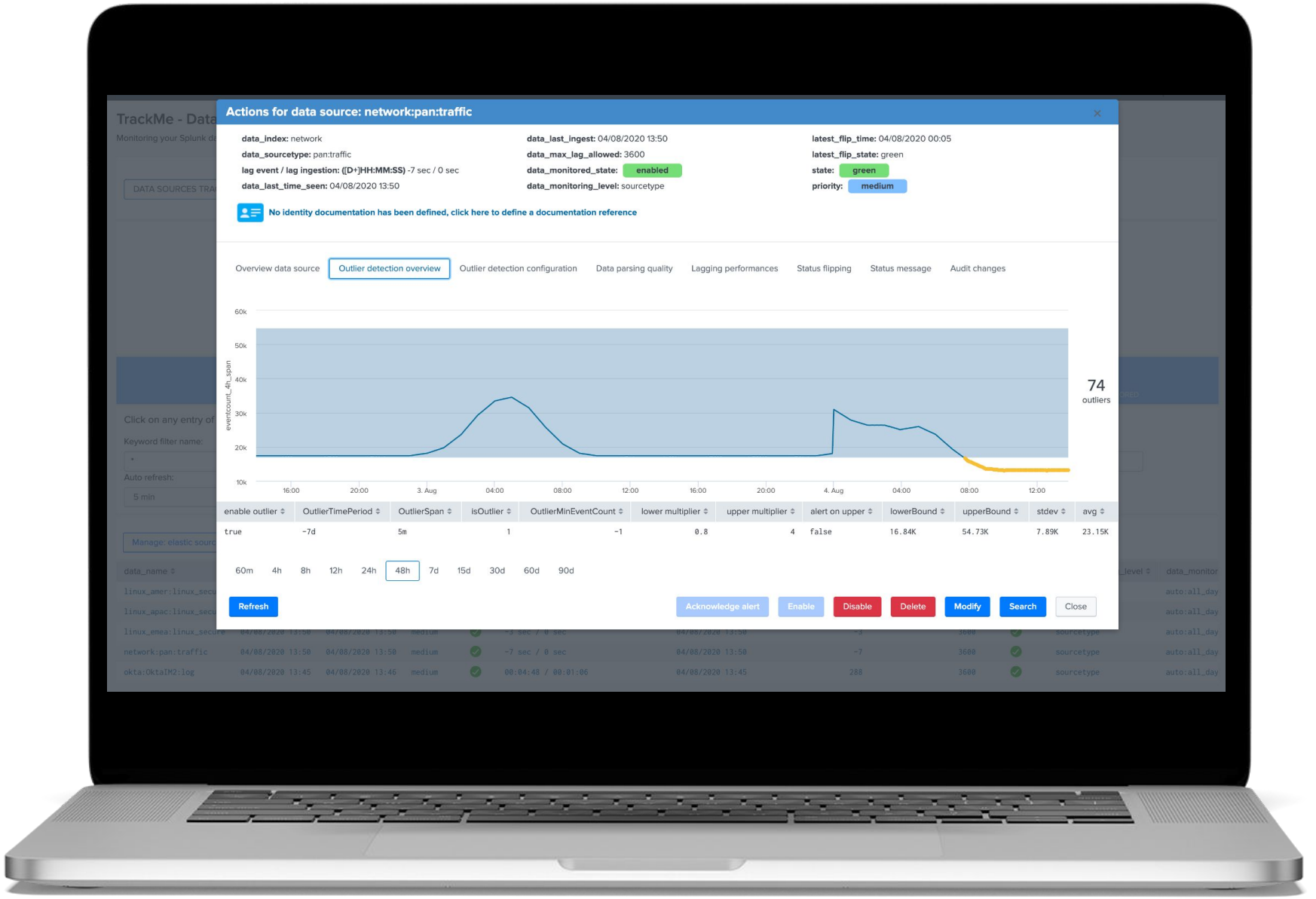
Many features are provided out of the box to cover all use cases

- TrackMe has many features that were designed to cover all of your needs, from common and standard data sources to very specific contexts, every Splunk customer is different!
- Main features are:
  - The delay and latency automated tracking, to alert when a source is late or suffering from latency
  - The MLTK based outliers detection, to alert when volumes become unusuals
  - The data sampling and event format detection, allowing to track format changes, inconsistent index time parsing, and even track for PII data!
  - The Elastic source concept, allowing to easily create a virtual data source of your own
  - The Smart Status, performing advanced investigation automatically on your behalf
- And more!

Outliers Detection

Easily detecting behaviour issues with ML that works!

TrackMe automatically records the **volume** of events linked to a data source, and applies simple **outliers based detection** to alert when the volume goes below or beyond

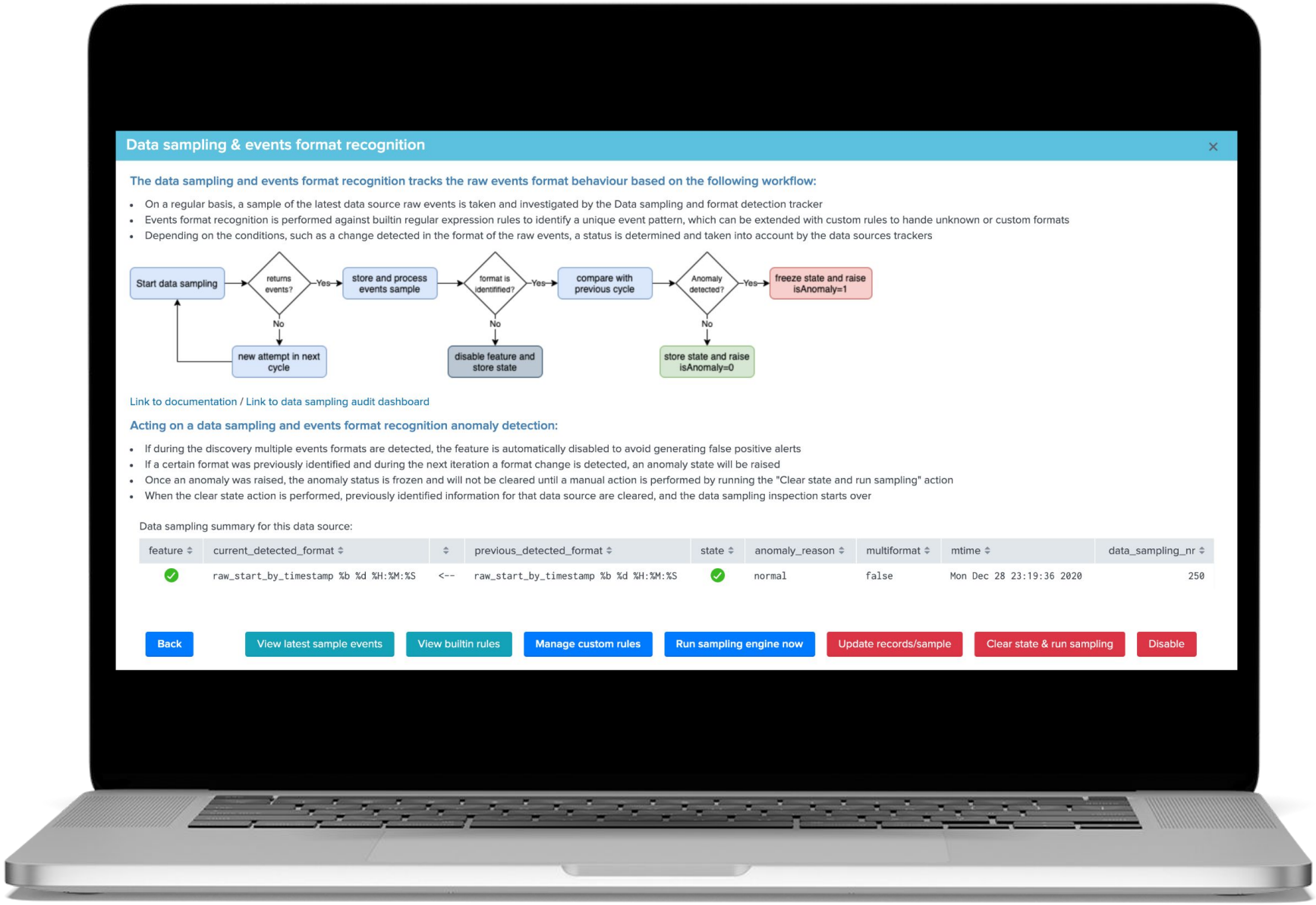


splunk> .conf21

Data Sampling and Event Format Recognition

Track quality issues automatically!

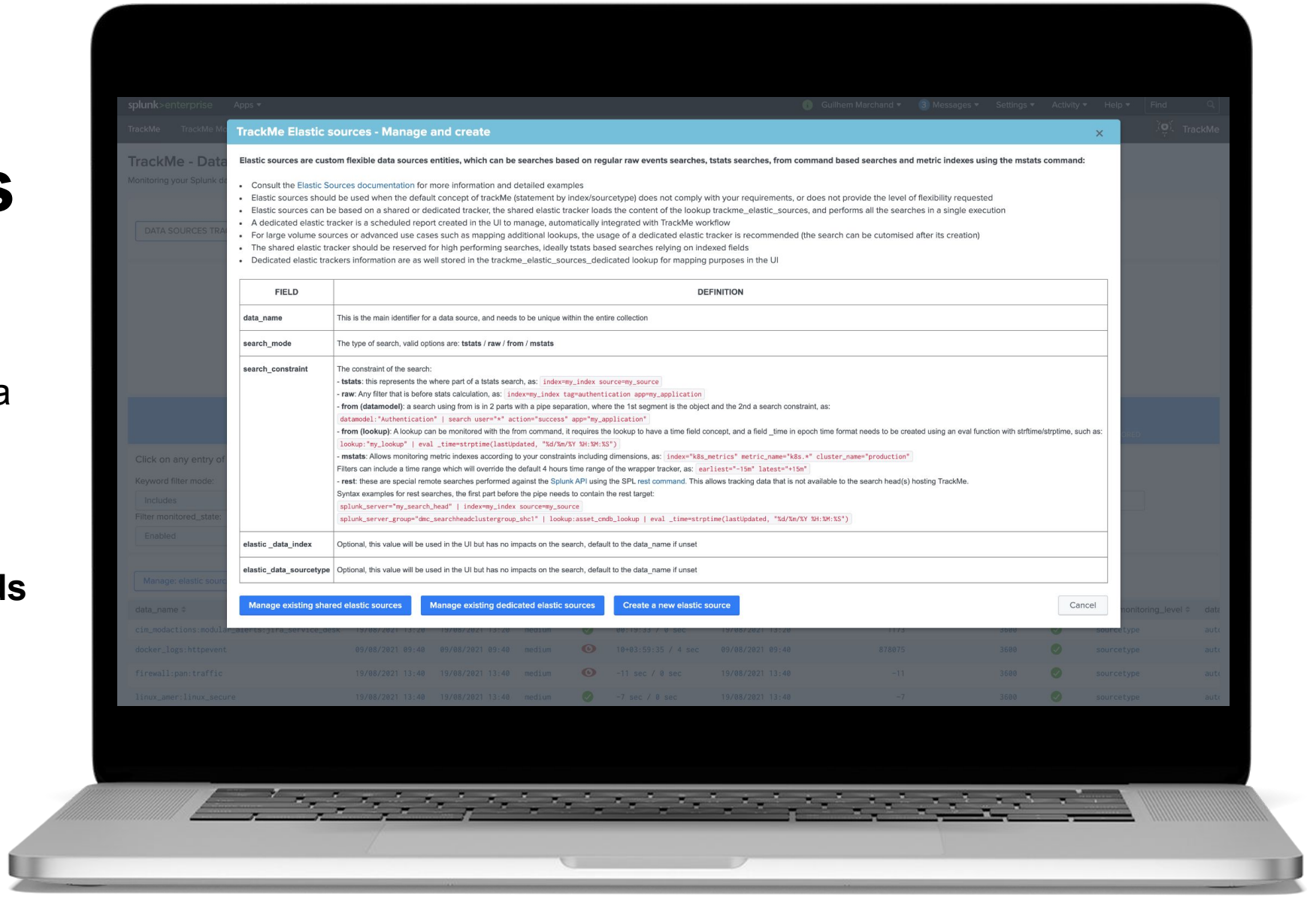
TrackMe provides out of the box a **powerful**, **automated** and **configurable** engine that detects and monitor event format changes, such as ingestion parsing issues that no one knows about!



Elastic Sources

Create custom virtual data sources of your own!

The out of the box concept of data sources has its limitations which might not fit your requirements, with Elastic Sources you can create any kind of entities, from relying on your own **indexed fields** to **lookups** monitoring

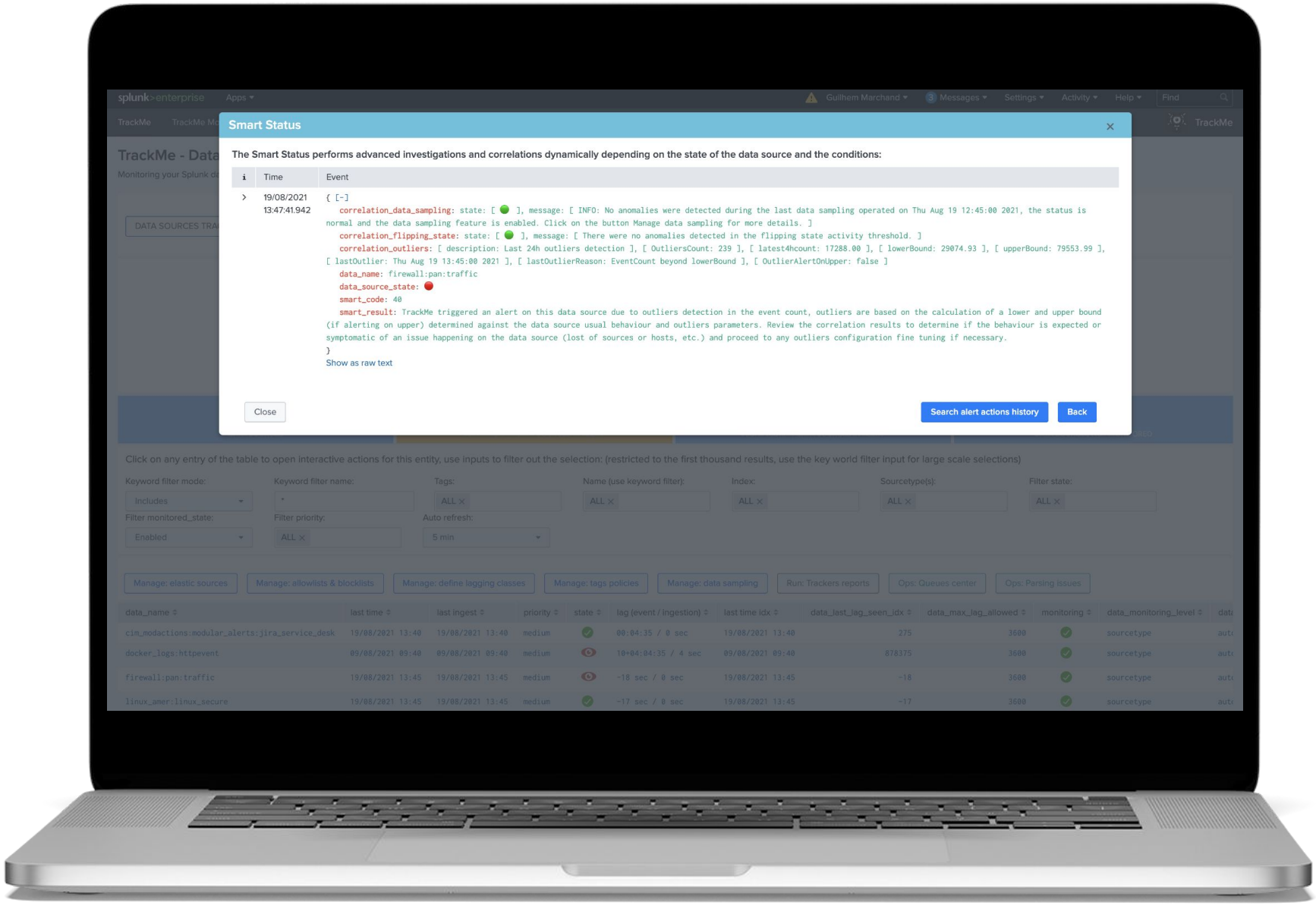


splunk> .conf21

Smart Status

Imagine how cool this would be to automate data source issues investigations?

This is what the **Smart Status** does, on-demand or automatically when an issue is detected, the Smart Status performs automated investigations to ease and speed the troubleshooting steps!



Getting the Best from TrackMe

ITSI integration, third party interactions

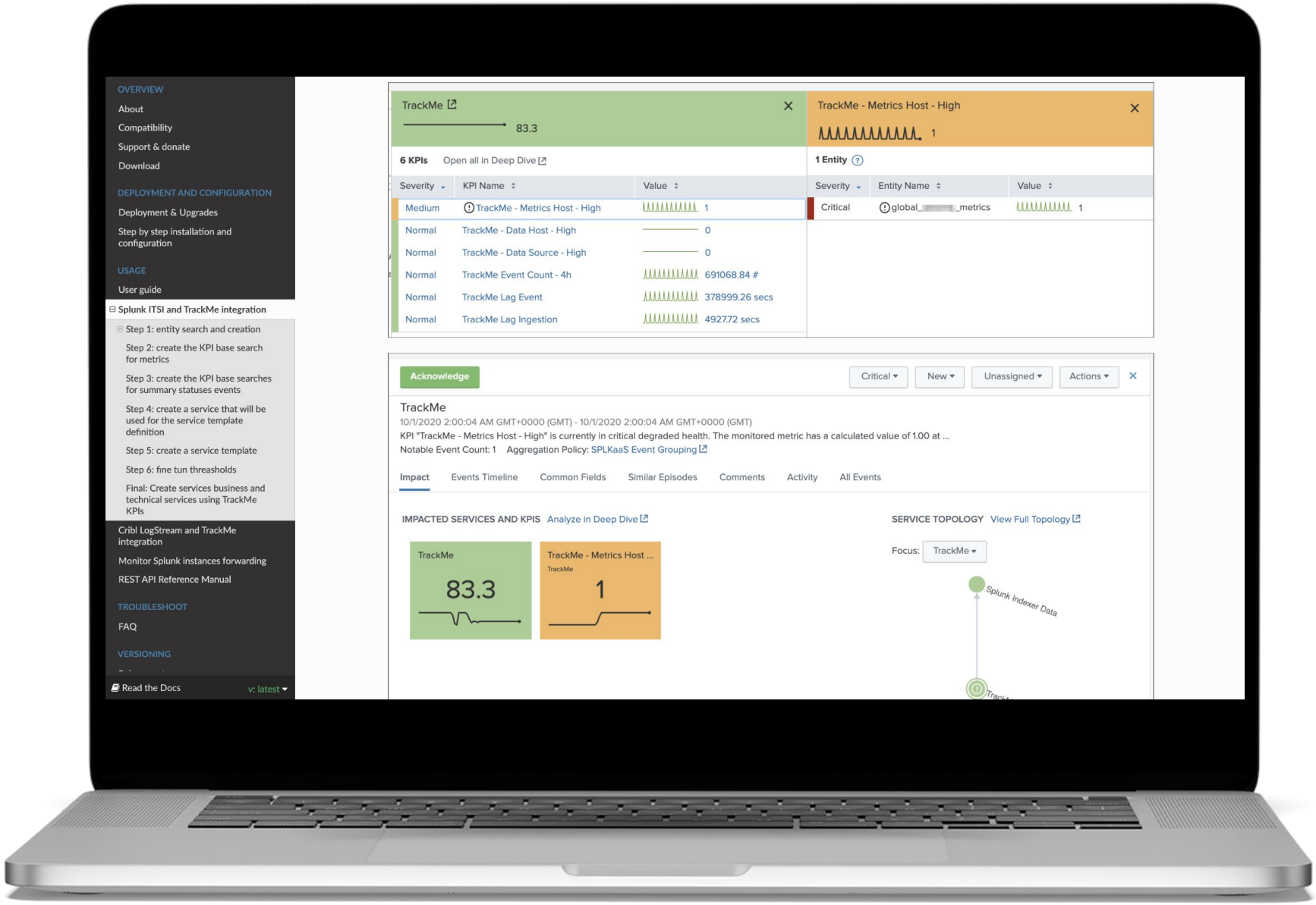
splunk> .conf21

TrackMe Loves ITSI!

If you are an ITSI customer, this is for you

You can very easily take great advantage of both products, to design a robust, performing and automated data source availability framework for your priceless data

https://trackme.readthedocs.io/en/latest/itsi_integration.html



splunk> .conf21

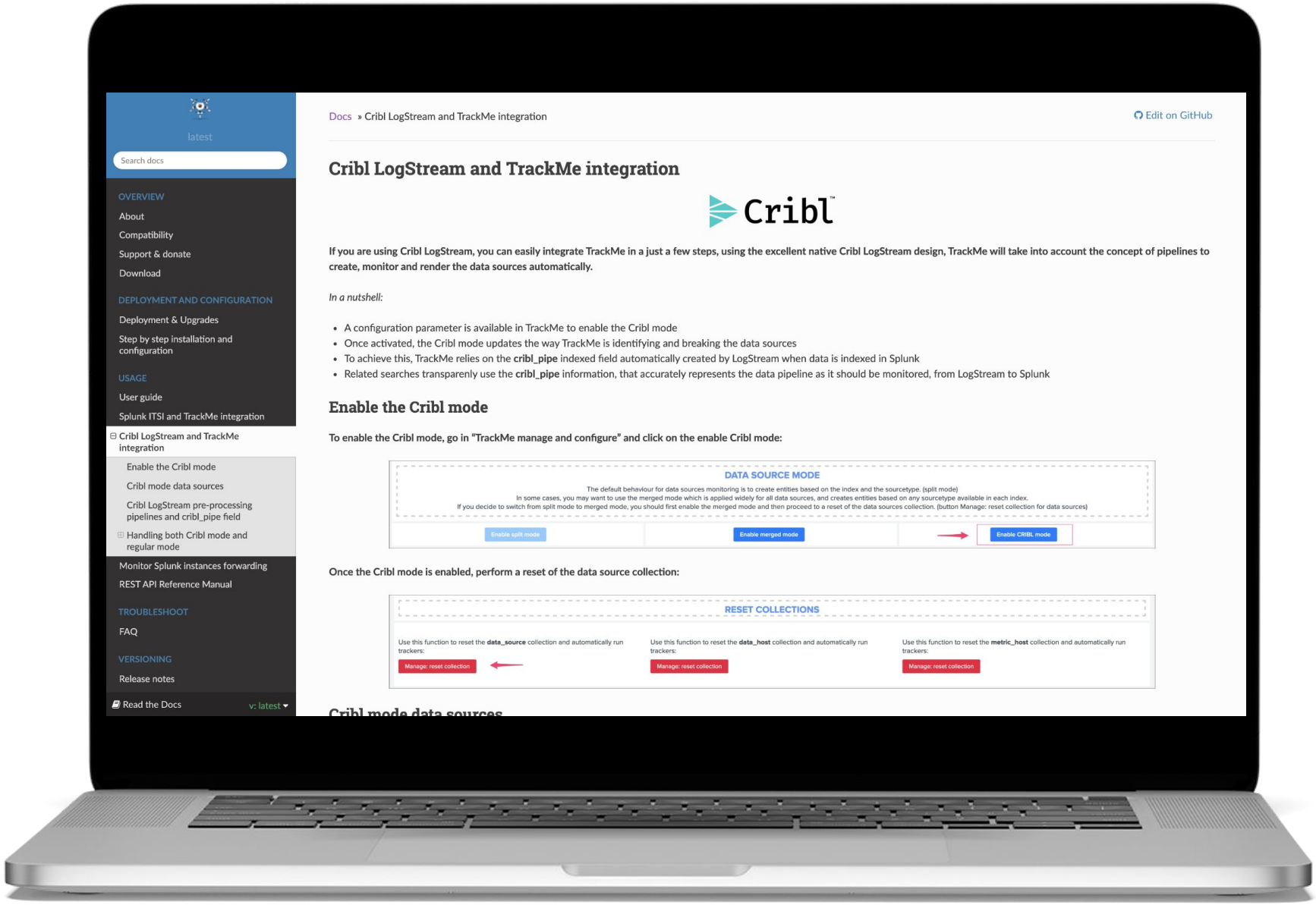
TrackMe and Cribl Logstream

Native Cribl integration

If you are using **Cribl Logstream**, then TrackMe makes the integration very easy.

In a single click, the app gets benefit from the product pipeline concepts to discover and define your data sources

https://trackme.readthedocs.io/en/latest/cribl_integration.html



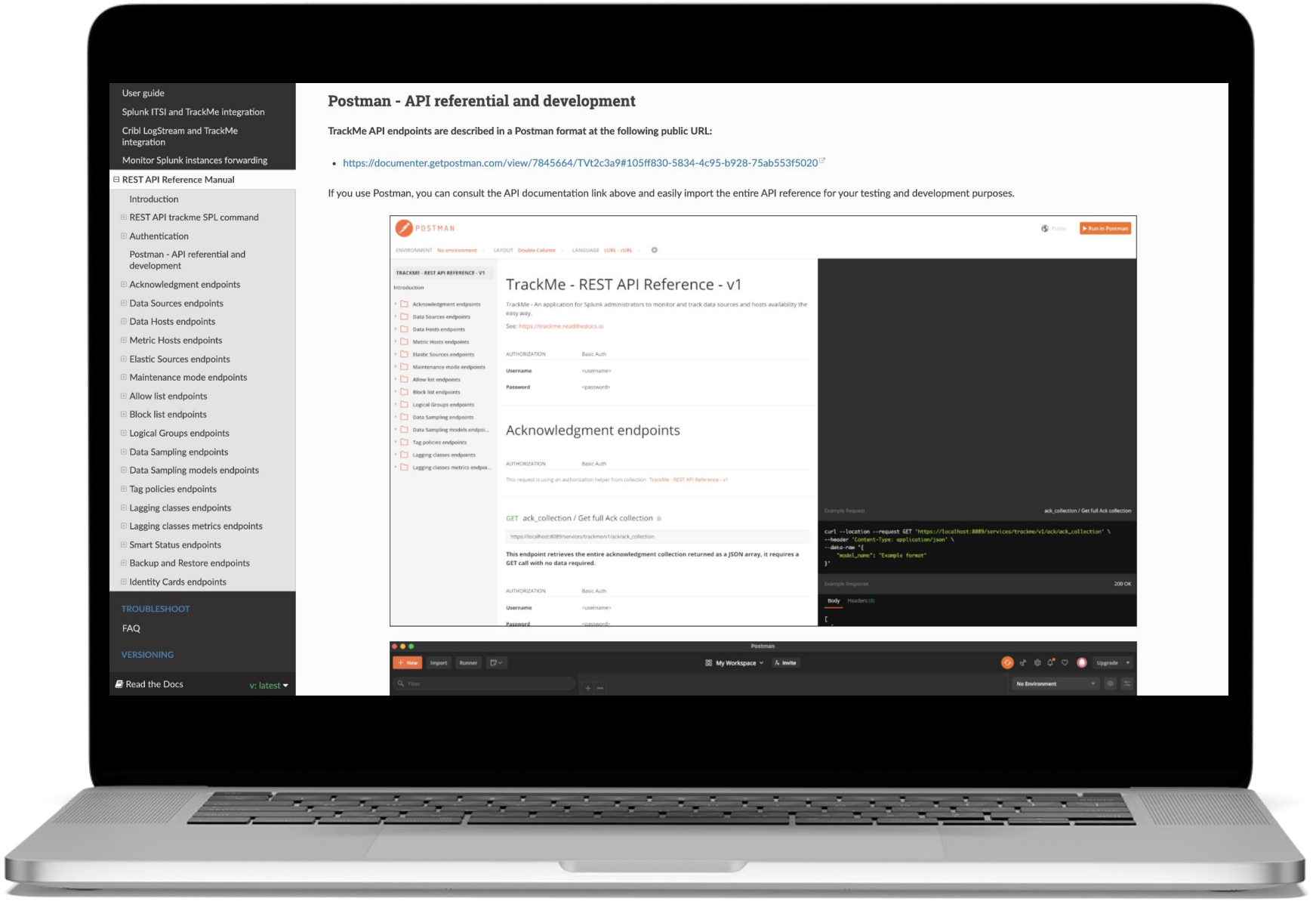
splunk> .conf21

TrackMe REST API

Interact with TrackMe!

TrackMe provides an extensive list of REST API endpoints, which you can interact with, in Splunk and from the outside World

https://trackme.readthedocs.io/en/latest/rest_api_reference.html



splunk> .conf21

Demo

Time for a TrackMe demo!

splunk> .conf21

About TrackMe!

Where to find it, where to start

Splunk Base:

https://splunkbase.splunk.com/app/4621

Documentation:

https://trackme.readthedocs.io

Thank You

Please provide feedback via the

SESSION SURVEY

splunk> .conf21