

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, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing 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. © 2021 Splunk Inc. All rights reserved.



Guilhem Marchand

Partner Professional Services | Octamis

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

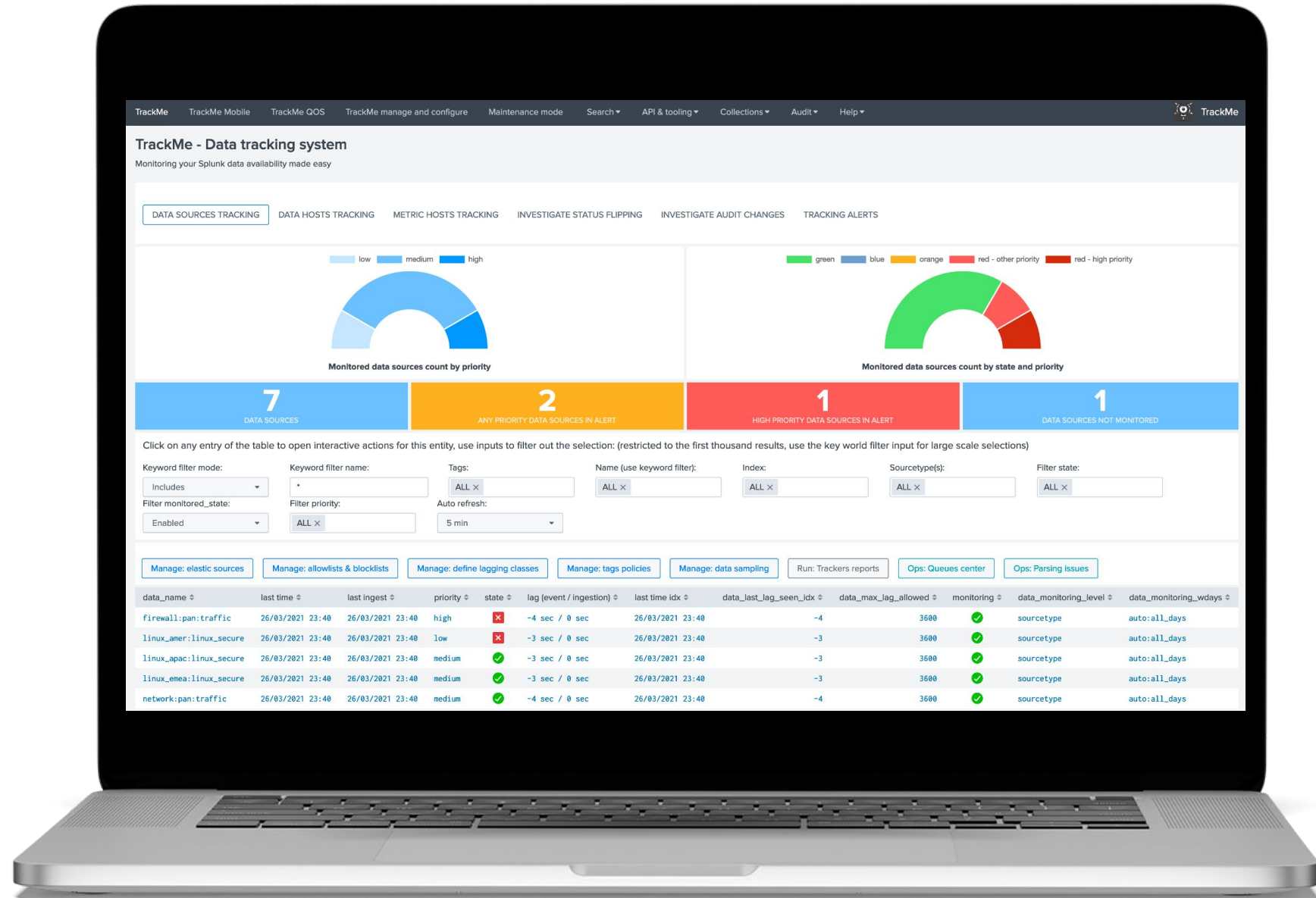


TrackMe!

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!



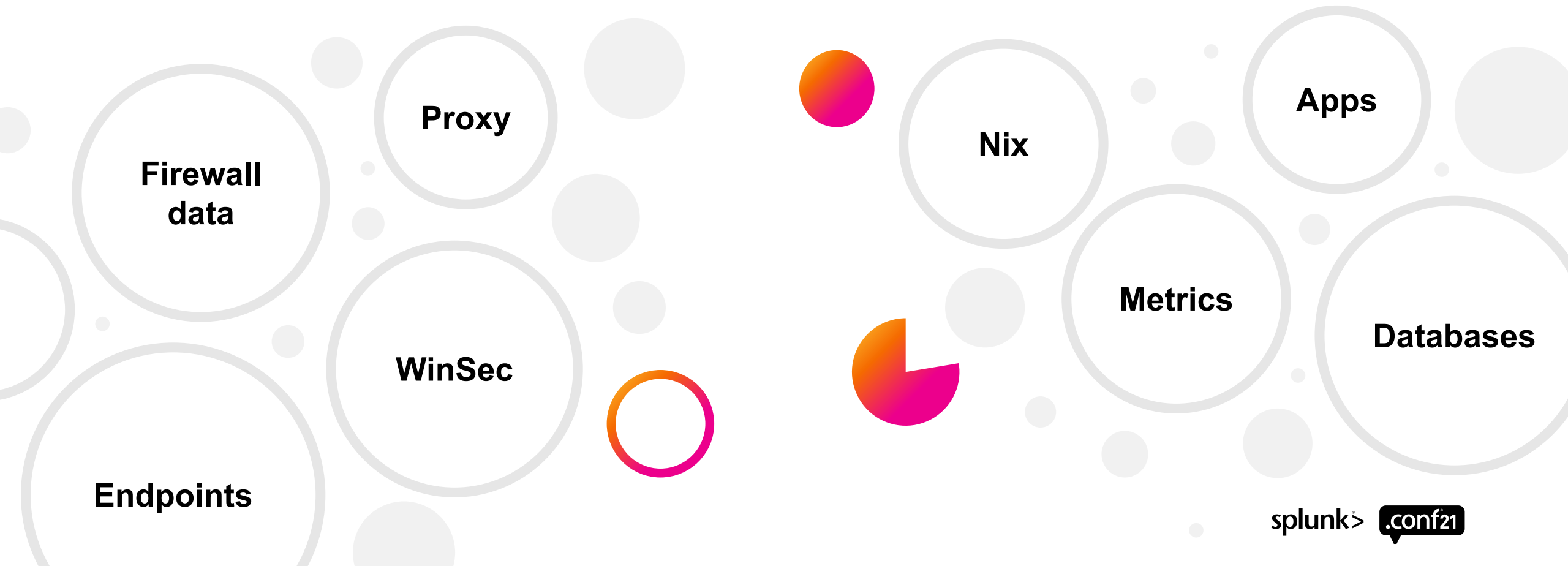


Monitoring Your Data Sources is Fundamental

At the root of TrackMe stand crucial questions too often neglected

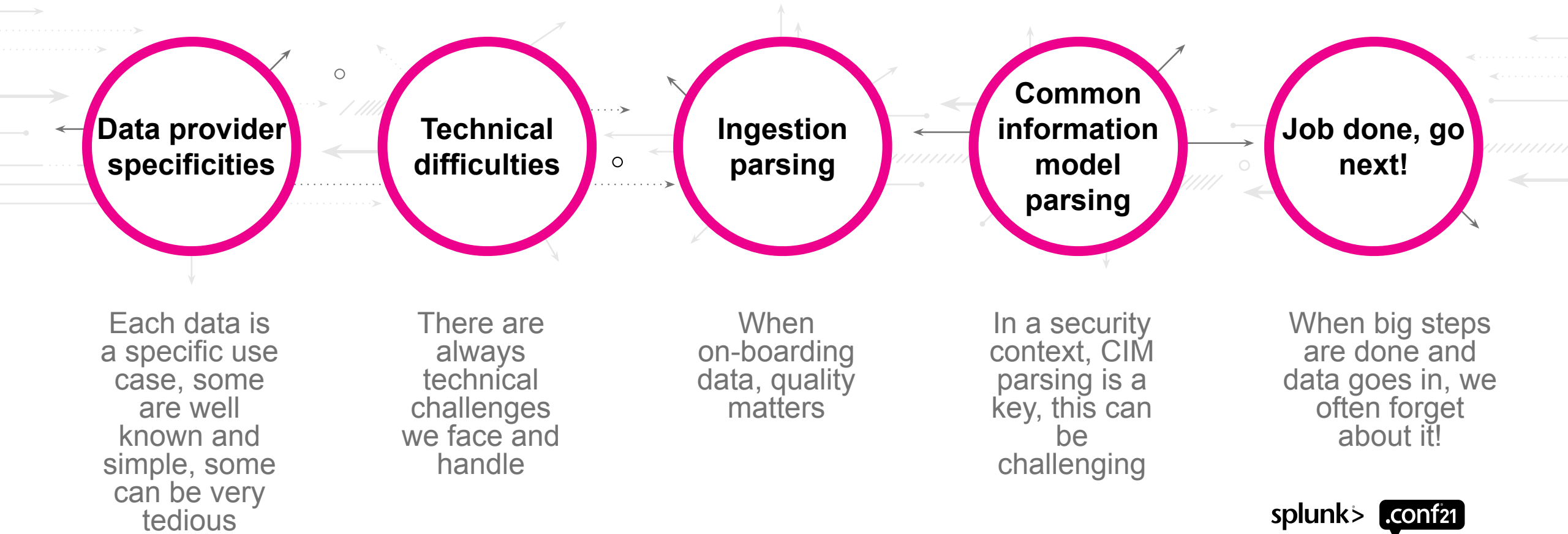
splunk> **.conf21**

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



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



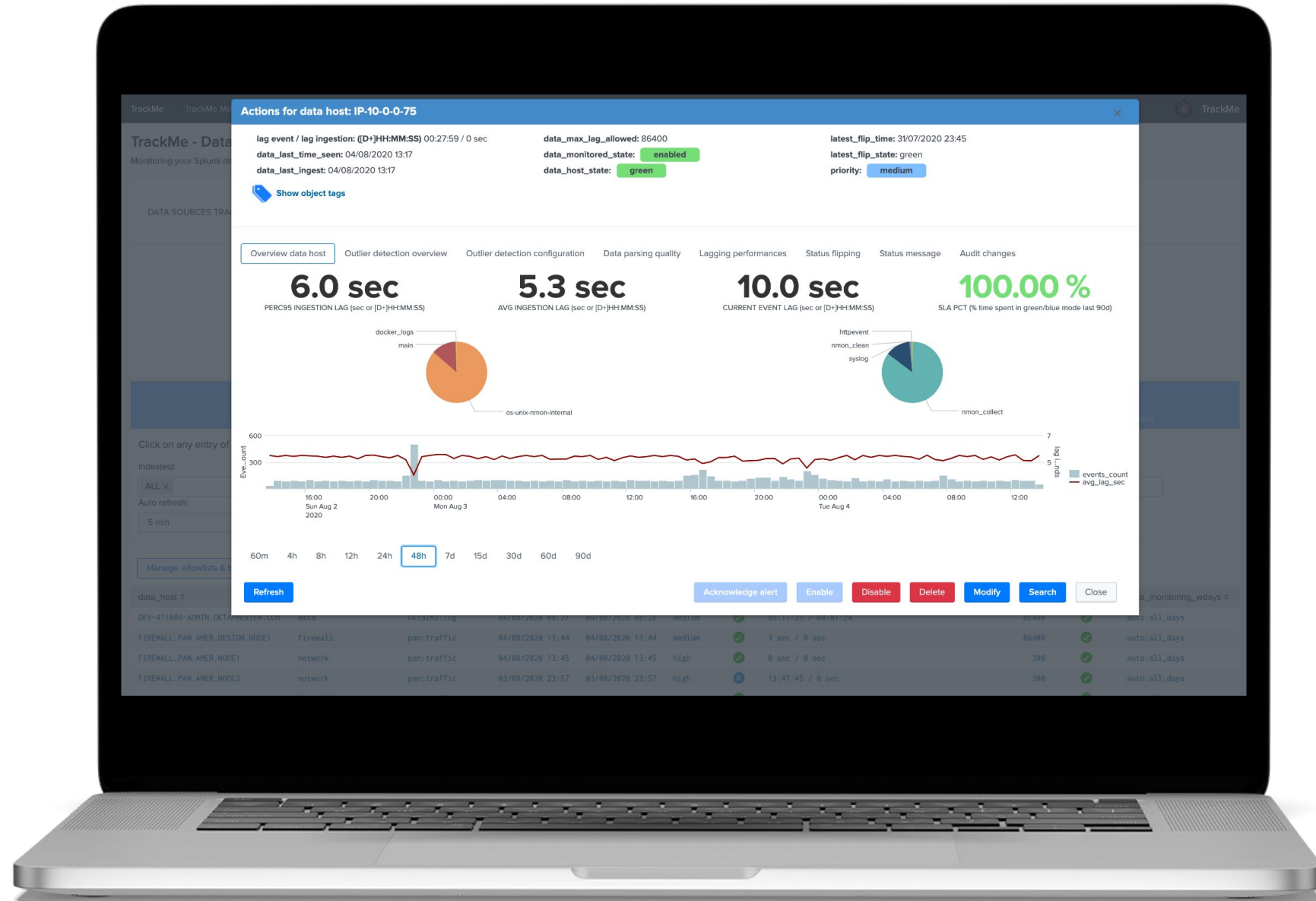
- TrackMe **discovers** and **maintains** every single data source in your environment automatically
- For **scaling** purposes, we use **tstats** based searches essentially
- Generic concepts are applied automatically, to handle **frequency** and expected **latency**
- **KPIs** are generated continuously (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





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



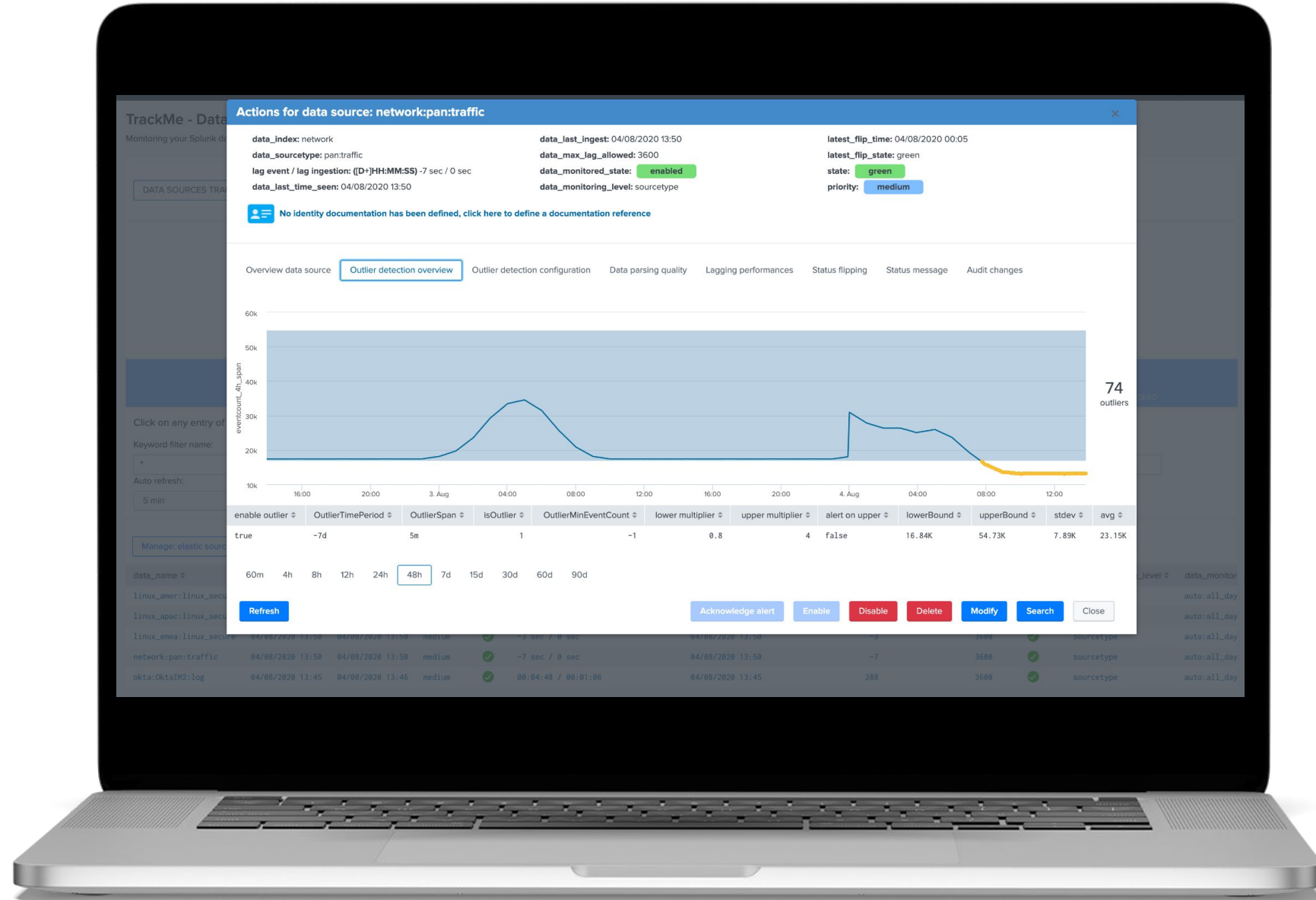
- TrackMe has many features that were designed to cover all of your needs, from common and standard data sources to very specific contexts, every Splunk customer is different!
- Main features are:
 - The delay and latency automated tracking, to alert when a source is late or suffering from latency
 - 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



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!

Data sampling & events format recognition

The data sampling and events format recognition tracks the raw events format behaviour based on the following workflow:

- On a regular basis, a sample of the latest data source raw events is taken and investigated by the Data sampling and format detection tracker
- Events format recognition is performed against builtin regular expression rules to identify a unique event pattern, which can be extended with custom rules to handle unknown or custom formats
- Depending on the conditions, such as a change detected in the format of the raw events, a status is determined and taken into account by the data sources trackers

```

graph TD
    Start[Start data sampling] --> Returns{returns events?}
    Returns -- Yes --> Store[store and process events sample]
    Returns -- No --> Next[new attempt in next cycle]
    Store --> Identified{format is identified?}
    Identified -- Yes --> Compare[compare with previous cycle]
    Identified -- No --> Disable[disable feature and store state]
    Compare --> Anomaly{Anomaly detected?}
    Anomaly -- Yes --> Freeze[freeze state and raise isAnomaly=1]
    Anomaly -- No --> StoreState[store state and raise isAnomaly=0]
    StoreState --> Start
  
```

[Link to documentation](#) / [Link to data sampling audit dashboard](#)

Acting on a data sampling and events format recognition anomaly detection:

- If during the discovery multiple events formats are detected, the feature is automatically disabled to avoid generating false positive alerts
- If a certain format was previously identified and during the next iteration a format change is detected, an anomaly state will be raised
- Once an anomaly was raised, the anomaly status is frozen and will not be cleared until a manual action is performed by running the "Clear state and run sampling" action
- When the clear state action is performed, previously identified information for that data source are cleared, and the data sampling inspection starts over

Data sampling summary for this data source:

feature	current_detected_format	previous_detected_format	state	anomaly_reason	multiformat	mtime	data_sampling_nr
✓	raw_start_by_timestamp %b %d %H:%M:%S	<-- raw_start_by_timestamp %b %d %H:%M:%S	✓	normal	false	Mon Dec 28 23:19:36 2020	250

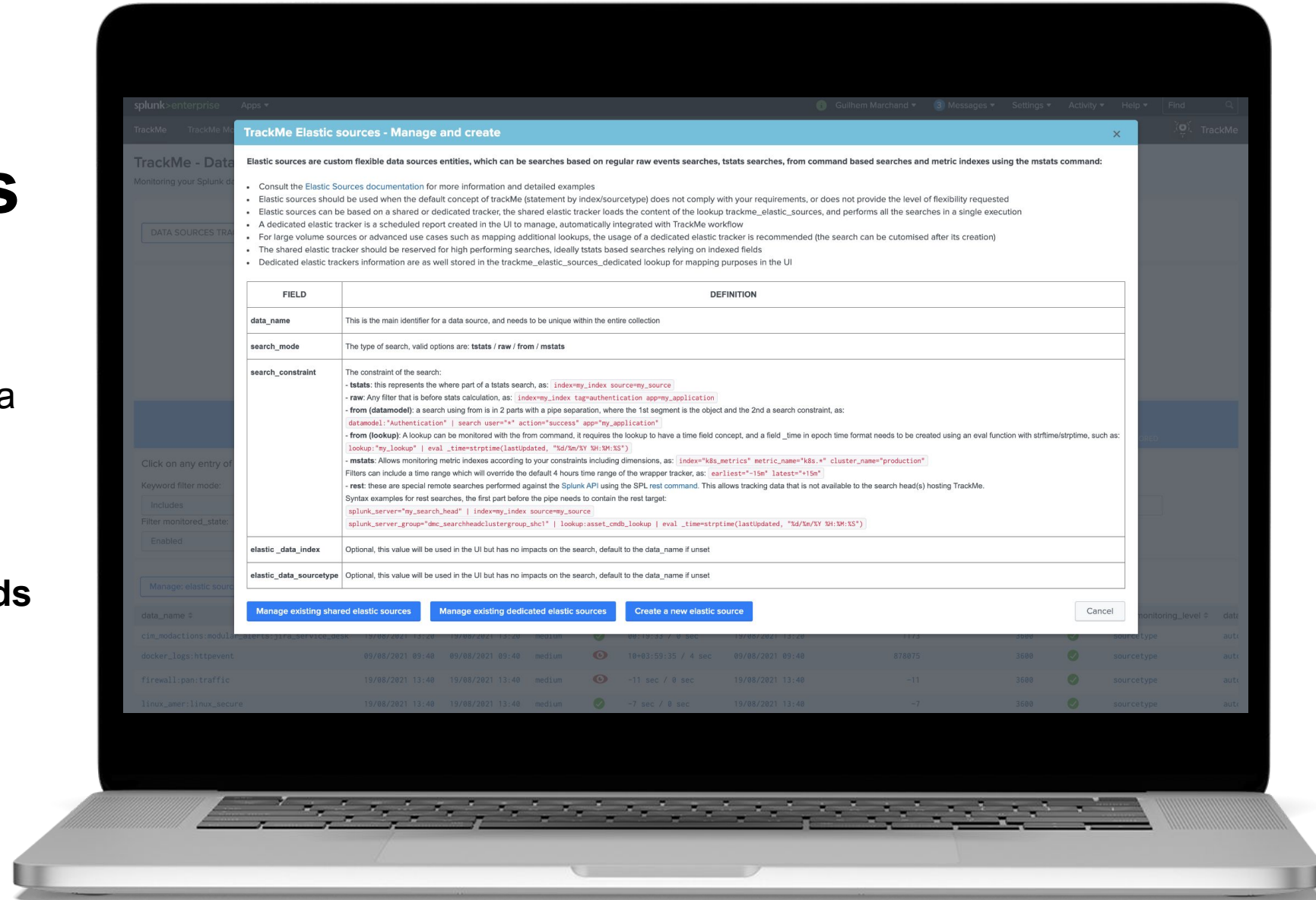
[Back](#)
[View latest sample events](#)
[View builtin rules](#)
[Manage custom rules](#)
[Run sampling engine now](#)
[Update records/sample](#)
[Clear state & run sampling](#)
[Disable](#)

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



TrackMe Elastic sources - Manage and create

Elastic sources are custom flexible data sources entities, which can be searches based on regular raw events searches, tstats searches, from command based searches and metric indexes using the mstats command:

- Consult the Elastic Sources documentation for more information and detailed examples
- Elastic sources should be used when the default concept of trackMe (statement by index/sourcetype) does not comply with your requirements, or does not provide the level of flexibility requested
- Elastic sources can be based on a shared or dedicated tracker, the shared elastic tracker loads the content of the lookup trackme_elastic_sources, and performs all the searches in a single execution
- A dedicated elastic tracker is a scheduled report created in the UI to manage, automatically integrated with TrackMe workflow
- For large volume sources or advanced use cases such as mapping additional lookups, the usage of a dedicated elastic tracker is recommended (the search can be customised after its creation)
- The shared elastic tracker should be reserved for high performing searches, ideally tstats based searches relying on indexed fields
- Dedicated elastic trackers information are as well stored in the trackme_elastic_sources_dedicated lookup for mapping purposes in the UI

FIELD	DEFINITION
data_name	This is the main identifier for a data source, and needs to be unique within the entire collection
search_mode	The type of search, valid options are: tstats / raw / from / mstats
search_constraint	The constraint of the search: - tstats: this represents the where part of a tstats search, as: <code>index=my_index source=my_source</code> - raw: Any filter that is before stats calculation, as: <code>index=my_index tag=authentication app=my_application</code> - from (datamodel): a search using from is in 2 parts with a pipe separation, where the 1st segment is the object and the 2nd a search constraint, as: <code>datamodel:"Authentication" search user="*" action="success" app="my_application"</code> - from (lookup): A lookup can be monitored with the from command, it requires the lookup to have a time field concept, and a field _time in epoch time format needs to be created using an eval function with strftime/strptime, such as: <code>lookup:"my_lookup" eval _time=strptime(lastUpdated, "%d/%m/%Y %H:%S")</code> - mstats: Allows monitoring metric indexes according to your constraints including dimensions, as: <code>index="k8s_metrics" metric_name="k8s.*" cluster_name="production"</code> Filters can include a time range which will override the default 4 hours time range of the wrapper tracker, as: <code>earliest="-15m" latest="+15m"</code> - rest: these are special remote searches performed against the Splunk API using the SPL rest command. This allows tracking data that is not available to the search head(s) hosting TrackMe. Syntax examples for rest searches, the first part before the pipe needs to contain the rest target: <code>splunk_server="my_search_head" index=my_index source=my_source</code> <code>splunk_server_group="dmc_searchheadclustergroup_shc1" lookup:asset_cmb_lookup eval _time=strptime(lastUpdated, "%d/%m/%Y %H:%S")</code>
elastic_data_index	Optional, this value will be used in the UI but has no impacts on the search, default to the data_name if unset
elastic_data_sourcetype	Optional, this value will be used in the UI but has no impacts on the search, default to the data_name if unset

Manage existing shared elastic sources

Manage existing dedicated elastic sources

Create a new elastic source

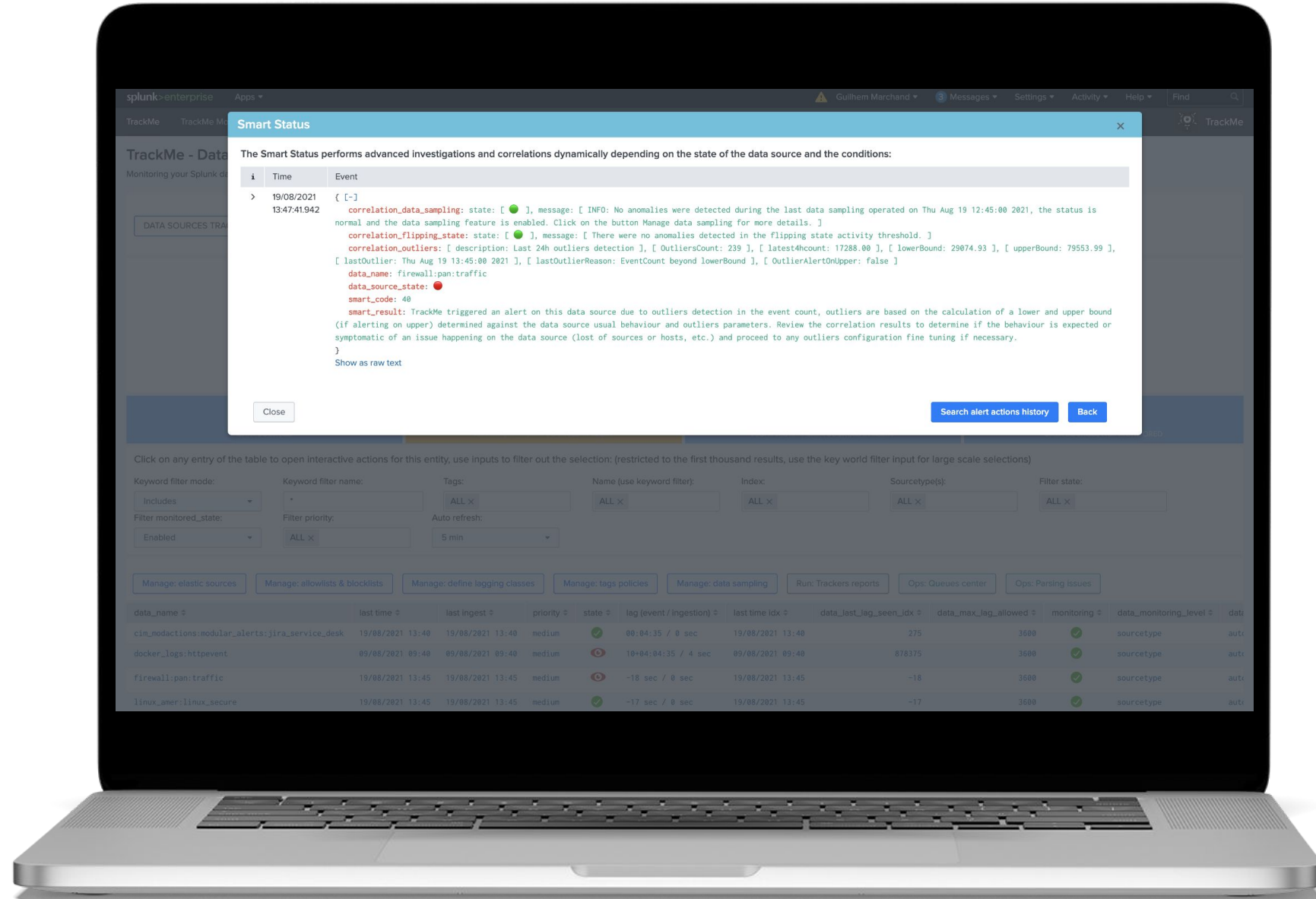
Cancel

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

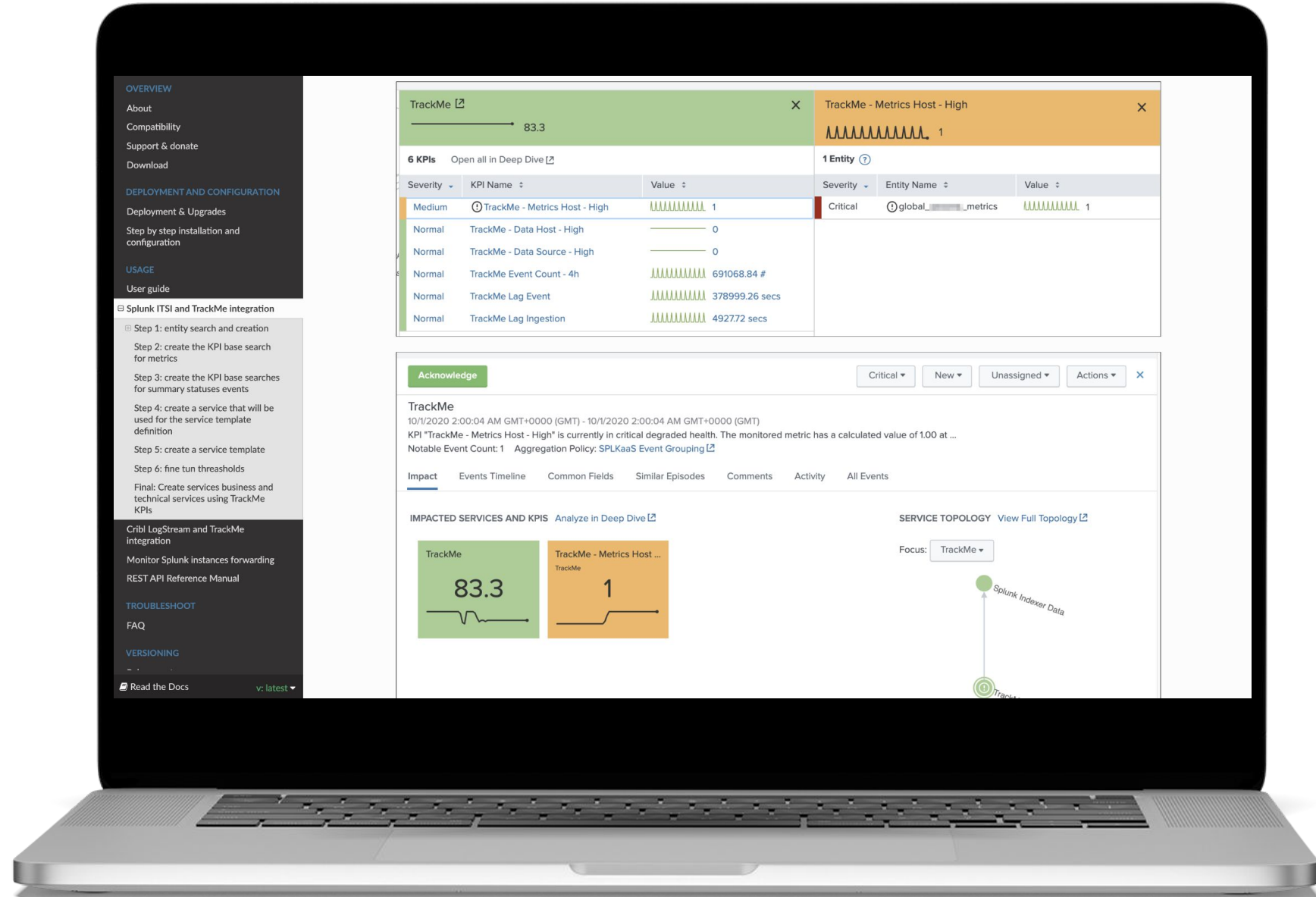
TrackMe Loves ITSI!

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



TrackMe and Cribl Logstream

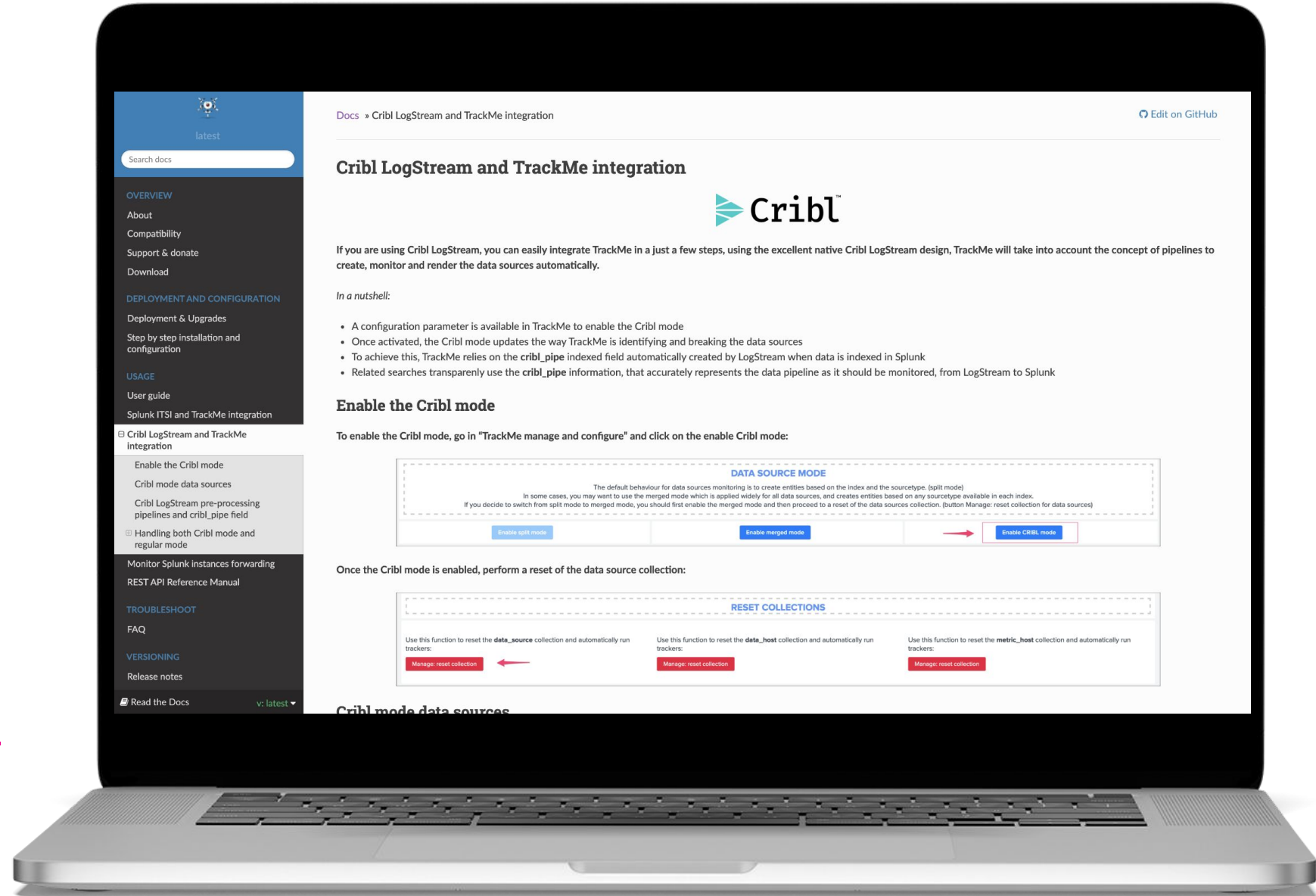
Native Cribl integration



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



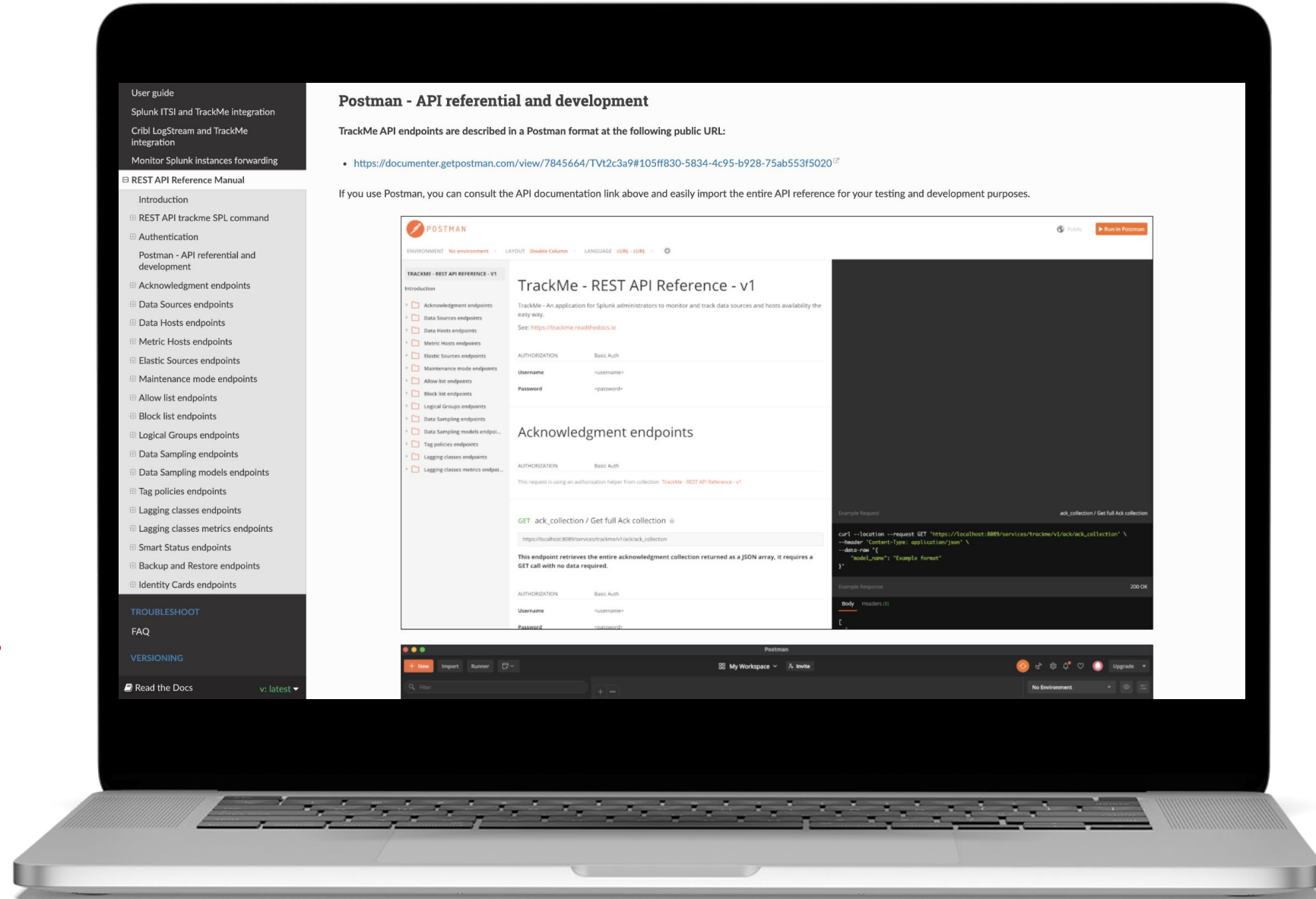
TrackMe REST API

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





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

