cloudera

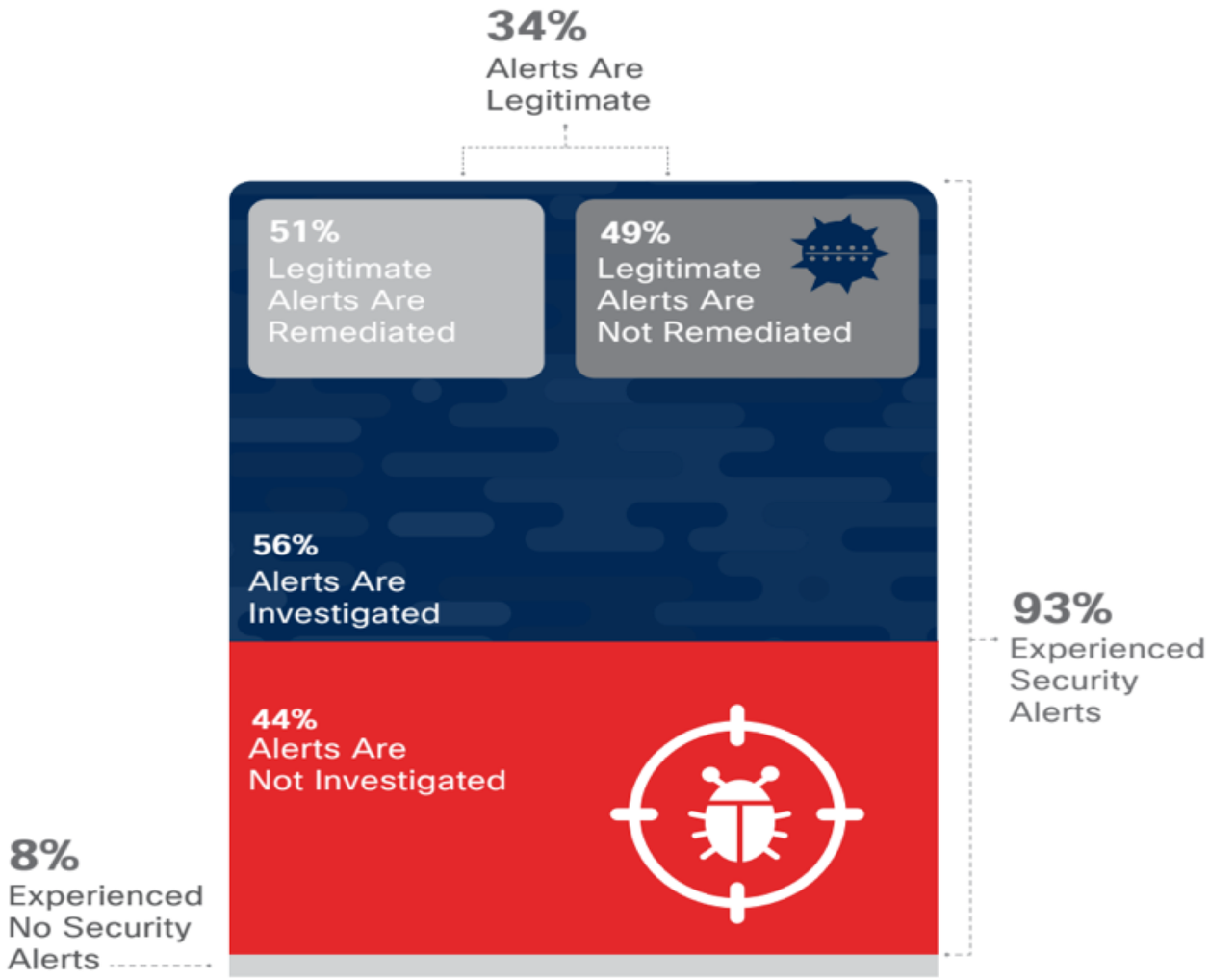
CLOUDERA CYBERSECURITY PLATFORM

Matthew Koehr

Solutions Engineer

Cloudera Government Solutions

HUGE PROBLEM IN ENTERPRISE CYBERSECURITY



source: Cisco cybersecurity report 2018

?

Not investigated **41%**

Investigated, but not remediated **26%**

Enterprises exposed to cyber threats **67%**

CYBERSECURITY IS A BIG DATA PROBLEM

Existing Cyber Security Solutions Don't Scale to the Challenge

82% of breaches happened in minutes

8 months is the average time an advanced security breach goes unnoticed

70%-80% of breaches are first detected by a 3rd party.

2016 Verizon Data Breach Investigations Report

Current security tools installed in the data center can't handle the volume of data & threats from everywhere

COMMON SECURITY OPERATIONS CHALLENGES

Too much to ingest

Rising data sources/attack vectors challenges staff to build & maintain data flows

Too much redundant ground work

Data architects and scientists are occupied by low value work of data gathering and cleansing

Too many disparate tools

Too hard to correlate security data in different systems (swivel chair analytics)

Too many alerts to process

Cybersecurity staff overwhelmed with alerts, spend all day doing alert triage

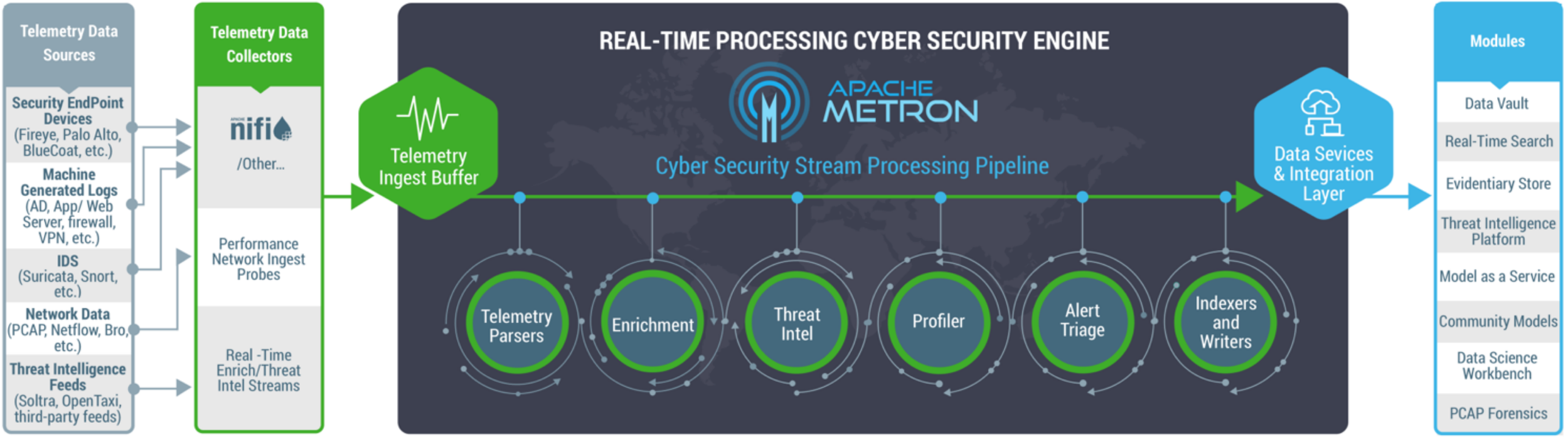
Too much data

Struggling with older SIEM (Security Incident & Event Management) tools that don’t scale and lack the analytics capability

Too much to handle

Company overwhelmed by building dedicated cybersecurity practices/platform or SOC (Security Ops Center) from the ground up

CYBERSECURITY PLATFORM, POWERED BY APACHE METRON

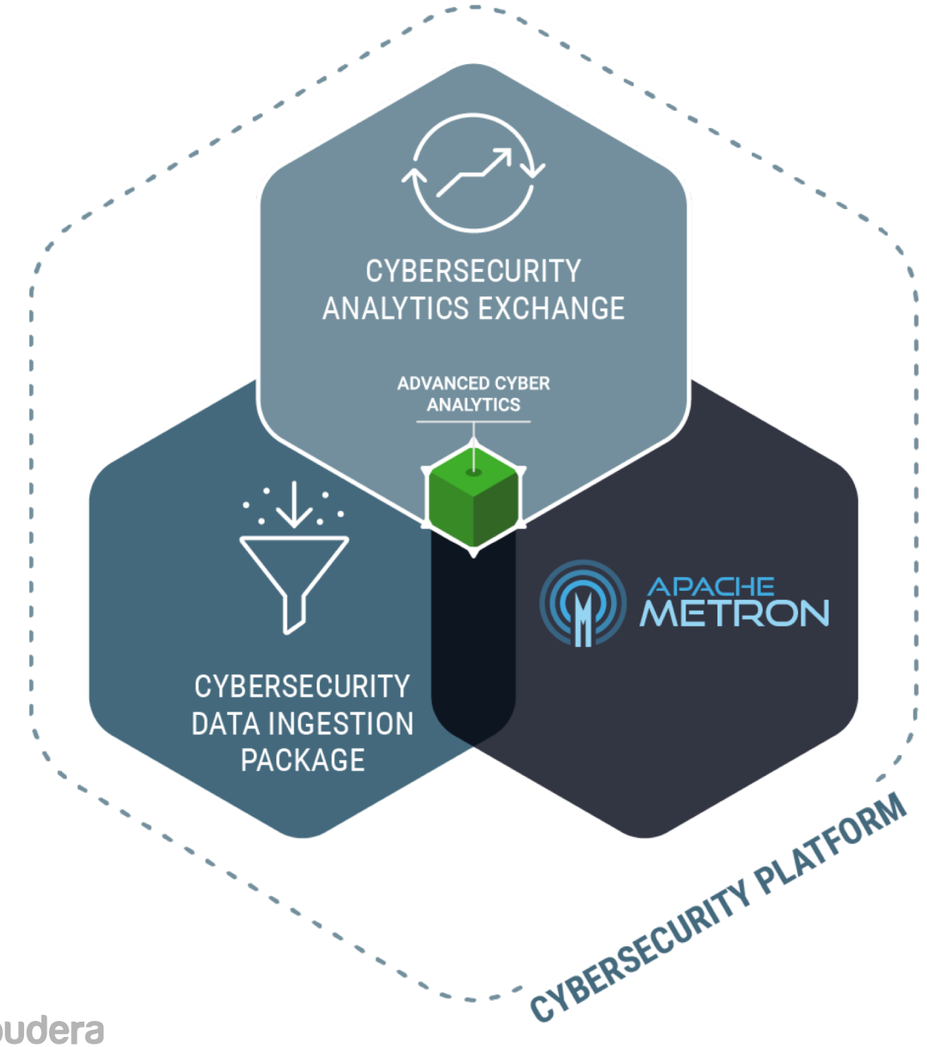


DATAFLOW for DATA-IN-MOTION

BIG DATA PLATFORM for DATA-AT-REST

APACHE METRON CAPABILITIES

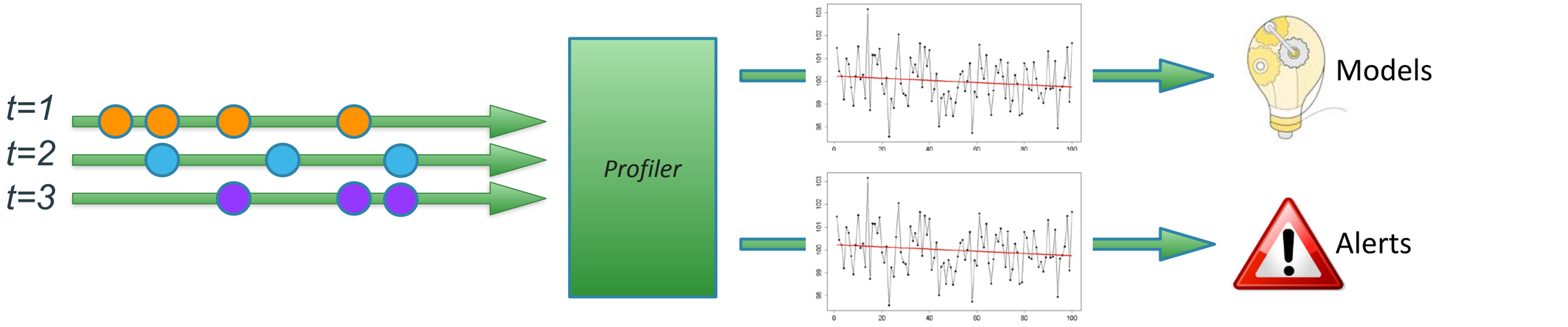
Accelerates organizations abilities to deploy & integrate advanced cybersecurity capabilities



Key Capabilities:

- Real-Time ingestion of application and system logs
- Real-Time cyber security dashboard and cyber workbench
- Real-Time ingestion, correlation and enrichment of PCAP and NetFlow telemetries
- Real-Time integration of Cyber security feeds
- Advanced statistical and machine learning models to detect cyber security attacks
- Integration with existing SIEMs and enterprise assets

PROFILER: ANOMALY DETECTION



Profile time series of data at each time period

Compare to statistical distribution

Alert when behavior outside normal range

- A generalized, extensible solution for extracting feature sets from high throughput, streaming data
- Generates a profile describing the behavior of an entity: a host, user, subset, or application
- A foundational component for both security model building and alerting in Metron

HOW WE HELP – HOW WE DO IT

We help companies create a security data lake or integrate one with existing SIEM environments. Companies **can retain data for longer and add real-time data ingestion, advanced analytics, and machine learning** to existing capabilities.

Variety = Complexity

- Ingestion Engines + Pre-Built Data Flows to simplify routing and processing of security data

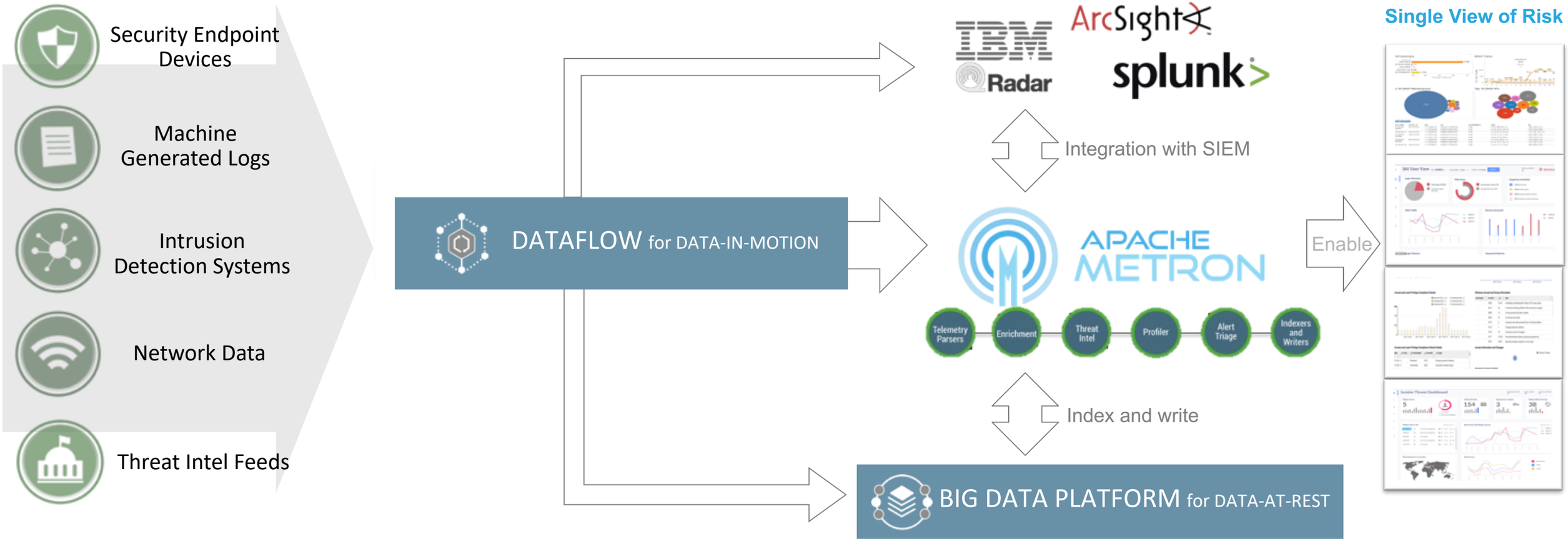
Volume = Cost

- Big Data platform to control cost via offload, distributed storage, and open source

Velocity = Constraint

- Real-time processing and enrichments provide reliable analytics results

SECURITY DATA FLOW OPTIMIZATION



Variety

of telemetry data sources

Velocity

in real-time ingestion

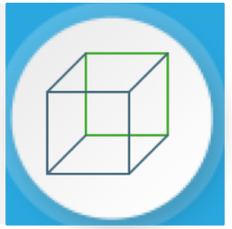
Volume

of security data storage & processing for insight

KEY DIFFERENTIATORS

100% open source big data technology – Open source data platform enables companies to ingest, manage and process ALL security data at massive scale.

Pre-built data ingestion dataflows– Metron is able to handle a wide variety of security data sources out of the box.



Big data behavior analytics and machine learning– Enable automation of threat detection with precision.

Flexibility– Gain flexibility with extended protection capabilities.

THANK YOU