cloudera®

A community based approach to fighting cyber threats

Rocky DeStefano
Cloudera Cybersecurity Subject Matter Expert

Morris Hicks
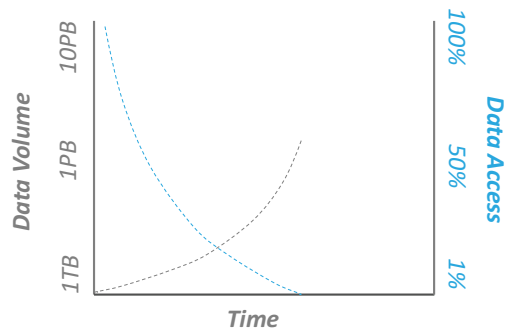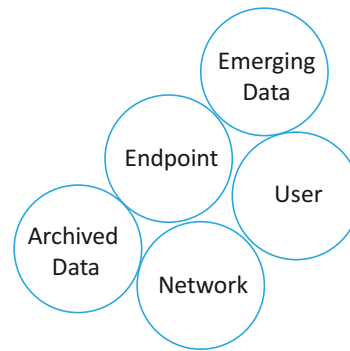Apache Spot Committer

1,000,000,000,000+

[events per day]

cloudera | intel

Stop Independently Solving Universal Challenges

Explosion of Data

Popular cyber platforms can not cost effectively scale to the volume and variety of modern data

Limited Enterprise Visibility

Only partial view of the enterprise limits analytics and slows investigations

IF (X) AND (Y)
THEN (Z)

Limited Analytic Processing

Difficult to deploy advanced machine learning detection capabilities

cloudera

Apache Spot
A community approach to fighting cyber threats.

The Value of Cloudera's Cybersecurity Solution
Based on Apache Spot

Faster time to incident investigation and response with comprehensive enterprise visibility

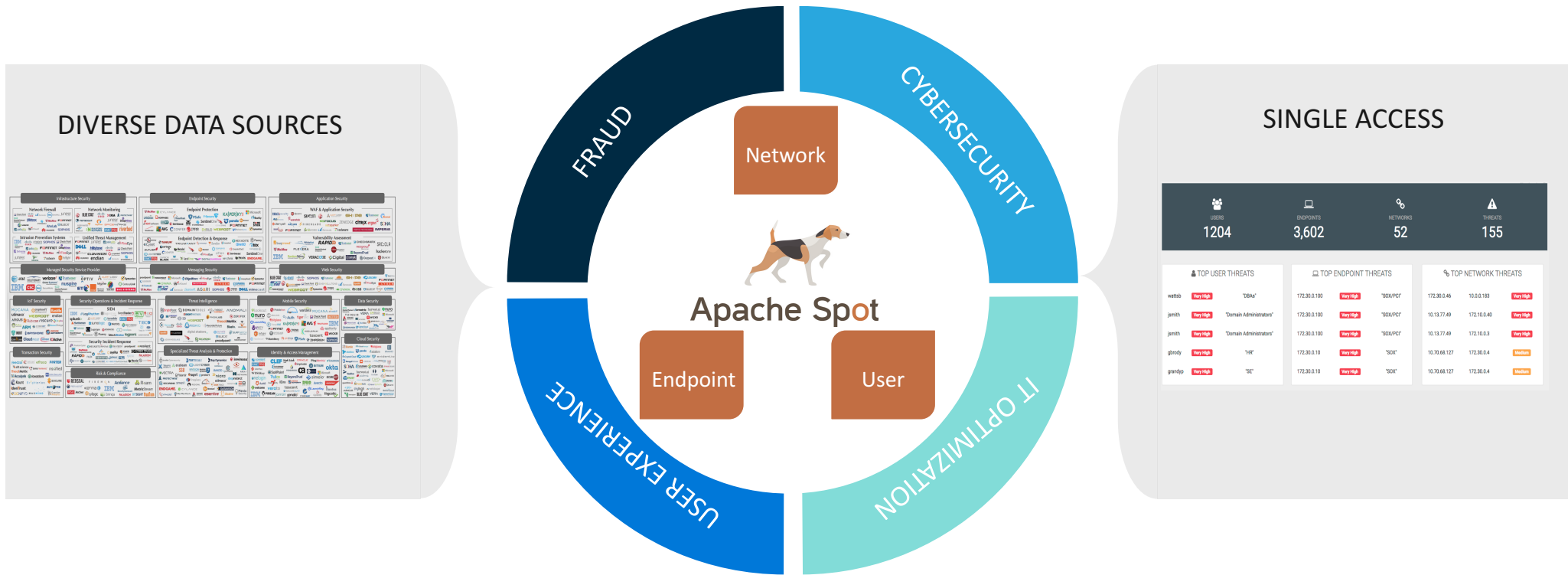**Detect advanced threats faster** via machine learning and artificial intelligence

Change the economics of cybersecurity with an open source platform that supports multiple LOB workloads

cloudera

Any Data from Any Source

Community Defined Open Data Models (ODM)

Many application on one shared data set and architecture

Packaged
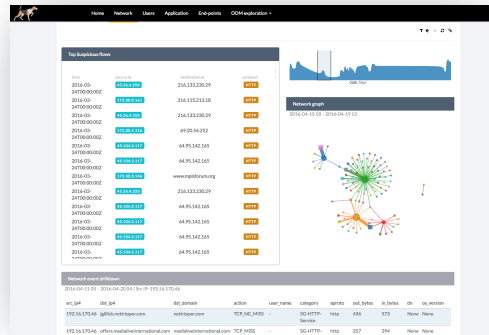

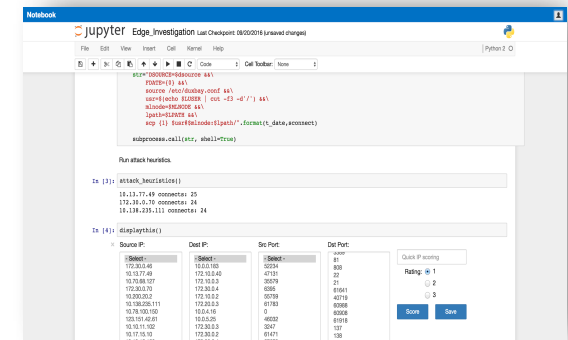Visualization & machine learning cybersecurity applications can share common data set & infrastructure

Open Source

Spot community is developing out machine learning (e.g. network threat detection)

Custom

Build custom applications & analytics using Cloudera without having to buy new infrastructure

cloudera

Integrate Cloudera with Existing Investments

Applications
- Packaged
- Apache Spot Algorithms
- Custom

Data and Analytic Management

SIEM

Cybersecurity Data Hub

- Analytic Processing *(Spark, Impala, Solr)*
- Apache Spot Open Data Models *(HDFS, Hbase, Kudu)*
- Ingestion *(Kafka, Flume, Streamsets)*
- Management, Governance, Security *(Cloudera Manager, Cloudera Navigator)*

(On premise or Cloud)

Data Sources
- Threat Intelligence
- Network
- User
- Endpoint
- Apache Spot Test Data

Large Scale Analytics

Search

Apache Solr

A Google search experience across all of your cybersecurity data

Visualizations

cloudera IMPALA

Large scale visualizations and SQL queries for descriptive and diagnostic analytics

Advanced Analytics

Apache Spark

Execute large scale machine learning queries against PBs worth of data for threat detection

cloudera

Demo

cloudera
Thank You