

A photograph of a modern building's interior hallway. The hallway is long and narrow, with a glass wall on the right side. A person is walking through the hallway, silhouetted against the light coming from the glass wall. The ceiling is dark, and the floor is also dark. The overall atmosphere is dark and industrial.

cloudera[®]

A community based approach to fighting cyber threats

Rocky DeStefano

Cloudera Cybersecurity Subject Matter Expert

Morris Hicks

Apache Spot Committer

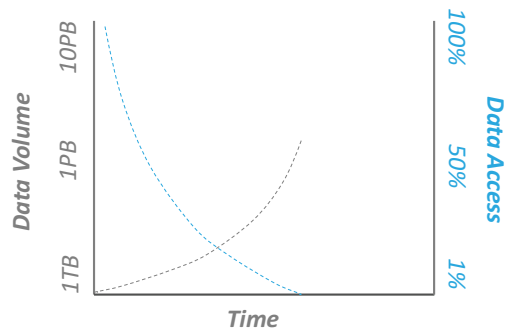


1,000,000,000,000+

[events per day]

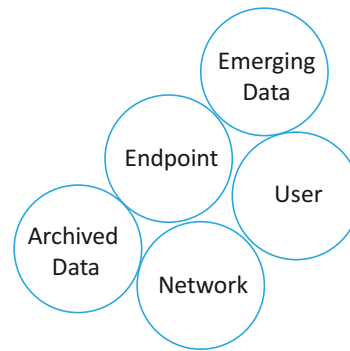


Stop Independently Solving Universal Challenges



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



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



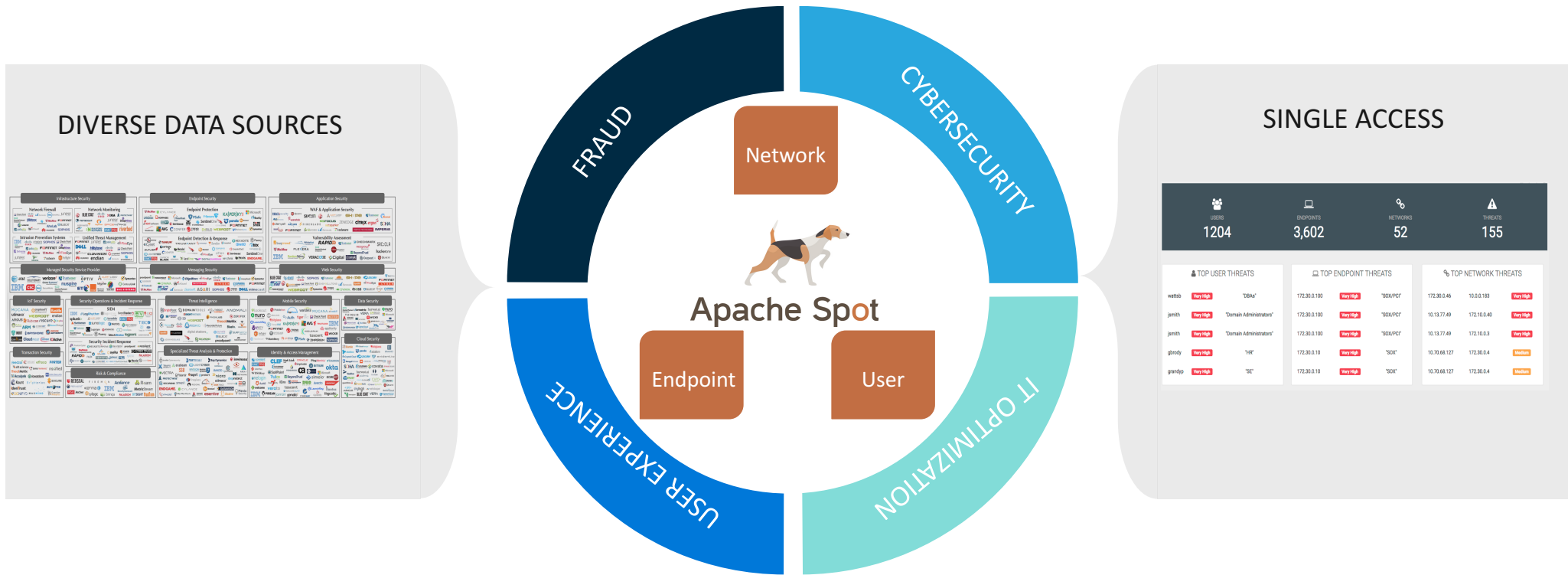
Change the economics of cybersecurity with an open source platform that supports multiple LOB workloads

Any Data from Any Source

The image displays a comprehensive grid of cybersecurity solutions, organized into 20 distinct categories. Each category is represented by a panel with a title and a collection of logos for leading companies in that space.

- Infrastructure Security:** Network Firewall (Check Point, Palo Alto, Juniper, Cisco, Fortinet, etc.), Network Monitoring (SolarWinds, Juniper, etc.), Intrusion Prevention Systems (Cisco, Fortinet, etc.), Unified Threat Management (Cisco, Fortinet, etc.).
- Endpoint Security:** Endpoint Protection (McAfee, Symantec, etc.), Endpoint Detection & Response (Snipe Systems, etc.).
- Application Security:** WAF & Application Security (Akamai, Cloudflare, etc.), Vulnerability Assessment (Qualys, Nessus, etc.).
- Managed Security Service Provider:** Includes logos for at&t, Verizon, Trustwave, etc.
- Messaging Security:** Includes logos for Proofpoint, Microsoft, etc.
- Web Security:** Includes logos for Blue Coat, Cisco, etc.
- IoT Security:** Includes logos for MOCANA, etc.
- Security Operations & Incident Response:** Includes logos for IBM, Splunk, etc.
- Threat Intelligence:** Includes logos for BrightPoint, etc.
- Mobile Security:** Includes logos for Lookout, etc.
- Data Security:** Includes logos for IBM, etc.
- Transaction Security:** Includes logos for Feedzai, etc.
- Risk & Compliance:** Includes logos for RedSeal, etc.
- Specialized Threat Analysis & Protection:** Includes logos for FortScale, etc.
- Identity & Access Management:** Includes logos for Okta, etc.
- Cloud Security:** Includes logos for Palo Alto, etc.

Community Defined Open Data Models (ODM)



Many application on one shared data set and architecture

Packaged

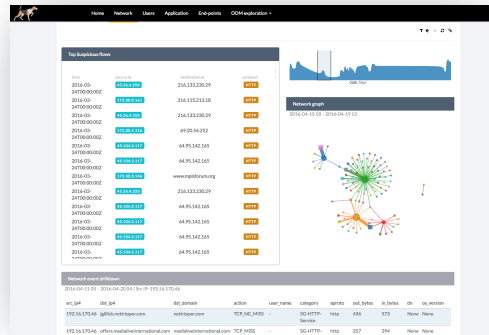


context relevant™

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

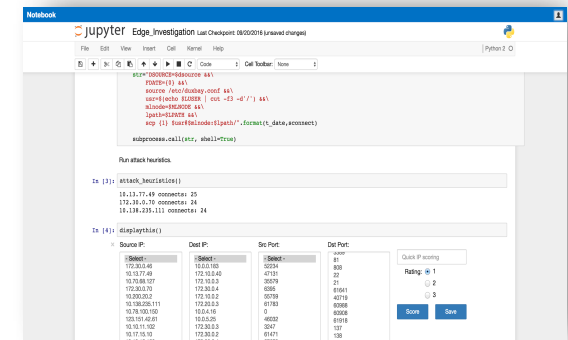
cloudera

Open Source



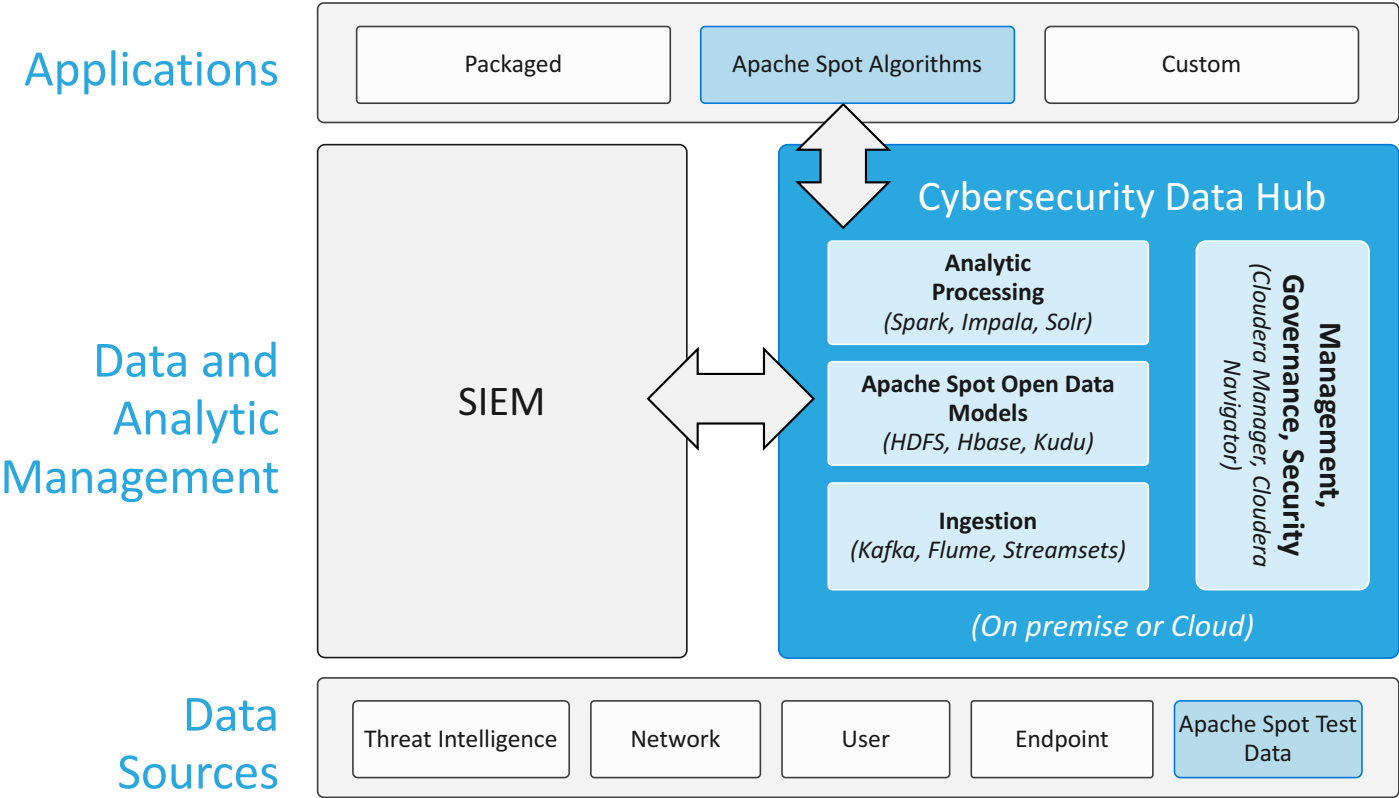
Spot community is developing out machine learning (e.g. network threat detection)

Custom



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

Integrate Cloudera with Existing Investments



Large Scale Analytics

Search



A Google search experience across all of your cybersecurity data

Visualizations



Large scale visualizations and SQL queries for descriptive and diagnostic analytics

Advanced Analytics



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

Demo

cloudera
Thank You