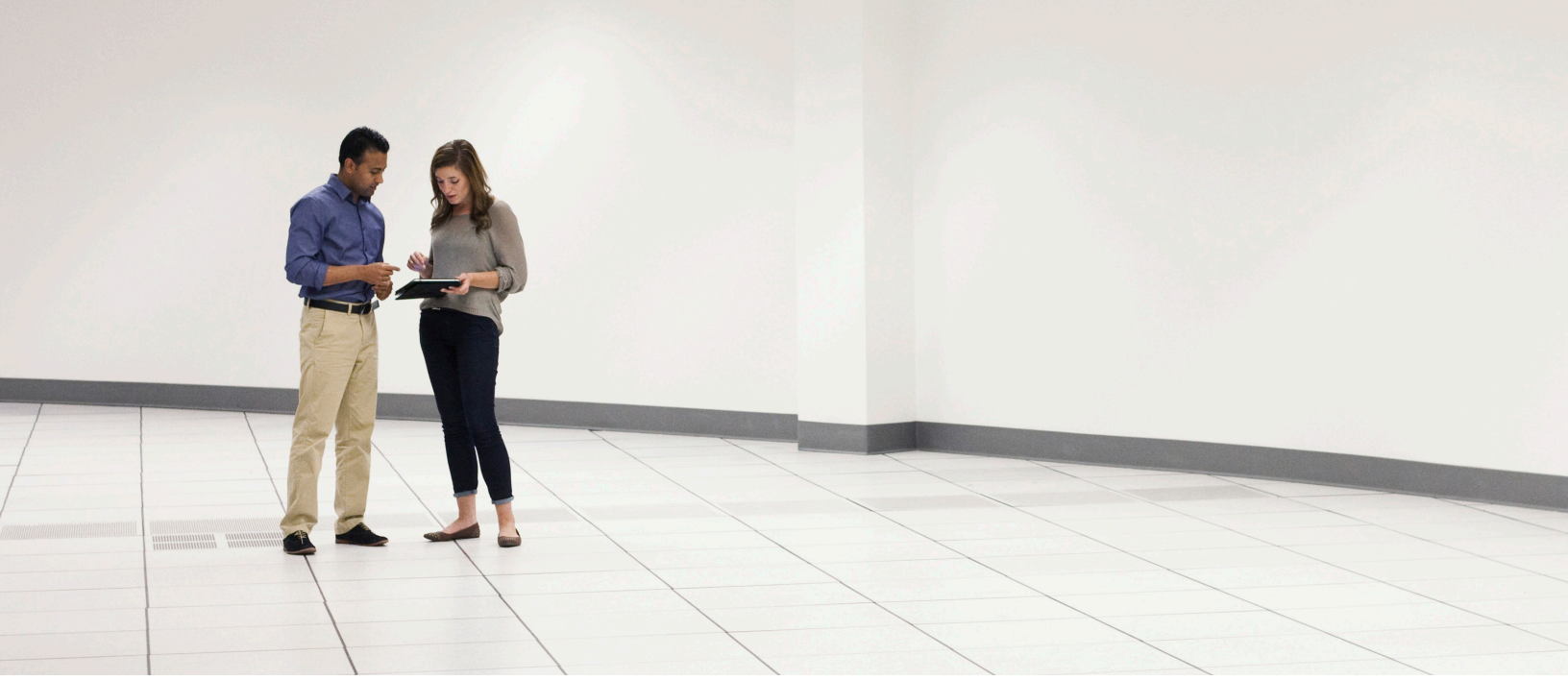

CYBRAICS

Harnessing AI to Change the Economics of Cybersecurity

"Cloudera's EDH provides a next-generation data and analytics management platform that can support the data volumes we work with and the breadth and depth of our cybersecurity analytics. This makes it possible for us to extract the full value of artificial intelligence by using all available data to assess cybersecurity risk and identify threats."

— Rob Kent, Vice President, Marketing and Business Development, Cybraics

Overview

The Cybraics nLighten platform combines big data analytics and artificial intelligence to deliver all-new cybersecurity capabilities. It fuses math, science, machine learning algorithms, and artificial intelligence into an unmatched capability for threat detection, while also reducing false positives dramatically. The platform is delivered to enterprises through an "as-a-Service" model, and depends on real-time access to huge volumes of data, made possible by a modern data platform from Cloudera.

Impact

Powered by Cloudera Enterprise and machine learning, Cybraics nLighten platform detects threats conventional cybersecurity solutions miss, and decreases customers' incident false positive rate from as much as 95 percent to less than five percent. This reduction significantly decreases the burden of triaging security alerts and directly cuts the time it takes to detect and respond to security incidents. Cybraics successes span the gamut across industries and threats—from helping utility companies protect their electric grids to uncovering nation-state cyberattacks against private enterprises.

Artificial intelligence (AI) is at the core of Cybraics' solutions, and this is made possible with Cloudera's modern data platform. As Richard Lovelace, senior vice president, Business Development at Cybraics explained, "Because Cloudera has a distributed architecture and distributed compute, it provides the horsepower that enables our analytics and artificial intelligence to more quickly detect the outliers, then correlate outliers with advanced threats."

Cybraics has seen a significant improvement in performance since it moved to Cloudera Enterprise. "When we first started, individual analytics would take up to eight hours to run against data," said Rob Kent, vice president of Marketing at Cybraics. "Now, with our Cloudera deployment and Intel® infrastructure, we can process all of our data in less than an hour, and those individual analytics can all run in minutes."

Cybraics believes in an open approach to cybersecurity solutions and has embraced Cloudera's work with the Apache Spot community to foster cybersecurity collaboration. "Today, cybersecurity is closed, but the only way that we are going to have any sort of impact on the persistent security threats is if we can collaborate and share," said Alan Ross, CTO of Cybraics and founder of Apache Spot. "With the community around Apache Spot's open data models, people have a centralized hub for security data. Spot's open data models enable us to plug in to that shared data set and infrastructure along with other ecosystem partners, so we can deliver results to our customers in less time."

cloudera®

cloudera®

Key Highlights

Industry
- Computer and network security

Location
- Headquarters: Atlanta, Georgia, USA

Business Application Supported
- Cybersecurity

Impact
- Reduction in incident false positive rate from 95 percent to less than five percent
- Decreased time to run individual analytics from eight hours to minutes
- Reduce resources required to triage security alerts
- Cuts time to detect and respond to security incidents

Data Sources
- Netflow
- SFlow
- Firewall
- Proxy
- Active Directory
- DNS
- VPN
- Virtually any security logs

Solution
- Modern Data Platform: Cloudera Enterprise
- Workloads: Data Science & Engineering
- Components: Apache Spark, Apache Spot
- BI & Analytics Tool: Custom
- ETL Tool: Talend

Business Drivers

Cybraics emphasizes three main issues in the security space based on customer input:

1. There are unknown and undetected threats everywhere.
2. The data volume for security teams to manage is untenable; there are more devices, attack surfaces, attack vectors, and vulnerabilities, and the volume of security alerts is increasing rapidly.
3. There is a proliferation of cybersecurity tools and point solutions, resulting in disconnected systems with limited visibility.

"We hear that as many as 70 percent of breaches happen because of previously unknown threats inside the environment," said Kent.

To address these issues, Cybraics required a platform that could support unprecedented data volumes and analytics complexity. "We have customers who are processing more than 40 terabytes of data a week," said Ross. "On our shared platform, we have multiple customers coming in, which is pushing into petabytes of data on a weekly basis. Then, we run our more than 30 unique, custom algorithms across all of this data. The advanced analytics required for this level of cybersecurity just can't be done within an appliance."

Solution

With Cloudera's modern data platform, Cybraics can analyze data to identify anomalies. Artificial intelligence then analyzes those anomalies to determine whether they are malicious. "Cloudera's EDH provides a next-generation data and analytics management platform that can support the data volumes we work with and the breadth and depth of our cybersecurity analytics," said Kent. "This makes it possible to extract the full value of artificial intelligence by using all available data to assess cybersecurity risk and identify threats."

Cloudera's platform enables each of Cybraics' three pillars—unsupervised analytics, its AI machine analyst called Janus, and the ability to deliver the platform as-a-Service. "We implement a technique we refer to as "Analytical Pluralism", meaning we run several sophisticated, computationally expensive analytics concurrently," said Ross. "Our analytics, which are largely based on unsupervised machine learning, but also include supervised and semi-supervised machine learning, excel on Cloudera's EDH and leverage Intel-based compute resources and memory to run effectively across the large data sets. Our custom algorithms can be applied to any data source we get. This covers the entire threat space and customer assets. Because our coverage is so broad, we can provide company-wide threat detection."

Cybraics' artificial intelligence layer, Janus, processes petabytes of data. With Cloudera's EDH, Janus can address the single biggest problem for cybersecurity—the velocity and volume of data generated in an enterprise environment. "The processing capability and power made possible by Cloudera running on Intel allows Janus to deliver on the promise of artificial intelligence," said Kent. "Janus's AI machine analyst component triages all analytics gathered and presents customers a list of what is benign and what demands attention. This shifts a significant portion of triage responsibility from man to machine, and allows the security team to focus on what matters, and achieve unparalleled scale."

The final challenge Cybraics needed to overcome was reducing the cost and complexity of deployment for customers. "To make these capabilities available to all enterprises we knew that we needed to deliver this as a service," said Kent. "Cloudera's EDH made this a reality, enabling us to implement the tooling, management, security, and automation to bring our vision to life."

About Cloudera

Cloudera delivers the modern platform for machine learning and advanced analytics built on the latest open source technologies. The world's leading organizations trust Cloudera to help solve their most challenging business problems by efficiently capturing, storing, processing and analyzing vast amounts of data. Learn more at cloudera.com.

cloudera.com

1-888-789-1488 or 1-650-362-0488

Cloudera, Inc. 1001 Page Mill Road, Palo Alto, CA 94304, USA