cloudera®

SOLUTION BRIEF

Deploying Cloudera's cybersecurity solution allows organizations to:

- Accelerate time to incident investigation and response with comprehensive enterprise visibility
- Detect advanced threats faster by applying machine learning and artificial intelligence to larger enriched data
- Change the economics of cybersecurity with an open source platform that supports multiple line of business workloads

Cloudera's Cybersecurity Solution

Cybersecurity has become the topic of conversation for organizations across every industry as the world continues to become hyperconnected. With the average breach costing $200 per lost customer record, and even more for lost intellectual property, organizations are looking for a new way forward. To add to the challenges, hackers are a highly collaborative group of individuals that share attack techniques every day. While enterprises, on the other hand, continue to operate individually with very little collaboration happening beyond basic threat intelligence sharing. We need to change as an industry.

Forward-thinking organizations have discovered a community-based approach to fighting cyber attacks leveraging Cloudera's open platform. Cloudera's cybersecurity solution, based on Apache Spot, enables anomaly detection, behavior analytics, and comprehensive access across all enterprise data using an open, scalable platform. Using the diverse open source community to accelerate shared innovations, while changing the economics of cybersecurity, allows organizations to come together to fight back against cyber threats.

Challenges

As the threat surface expands the increased number of sophisticated attacks continues to expose organizational vulnerabilities. The tools available to security operations centers (SOCs) are not built for the modern adversary operating in the hyper connected world. Challenges range from responding to suspicious activity with limited context, discovering advanced threats buried in billions of event, and understanding the true business risk associated with a user or entity.

Long Investigation & Response Time

Reducing the mean time to incident resolution (MTTR) is a key performance indicator of the efficiency of any SOC and incident response team. Factors pushing the MTTR up can be attributed to the fact that historic data is made unreachable due to archives, necessary data is scattered amongst multiple applications, and important contextual data is not even being collected in the first place. This limited enterprise visibility not only pushes the MTTR up, but also makes it impossible for incident responders to have complete confidence in their classification of suspicious activity.

Detecting Unknown Threats

Traditional cybersecurity applications, like security information event management systems (SIEMs), are notorious for their high false positive rates due to their signature and correlation based techniques (if<A>and<B>then<C>). The detection capabilities are fantastic for known threats, but as the threat landscape gets more complex, hackers find ways around these rules. Even if SOCs want to deploy large scale anomaly detection or behavior analytics via machine learning on enriched data, it's impossible to run these analytics due to the processing limitation of traditional technology.

Understanding the True Business Risk

CISOs have the critical and highly difficult job of balancing risks with the current resource constraints of their enterprise. As the compliance landscape continues to change, and the next major attack always around the corner, security operations centers need to truly understand the risk associated with every user and entity. Understanding this risk to properly invest resources prior and even during an attack will allow enterprises to better mitigate overall cyber risk.

Challenges by Role

CISO – Future proofing a strategy while balancing overall cyber risk exposure with enterprise constraints is not a trivial task

Security Engineer – Adding new data streams while scaling and integrating applications causes technology constraints

Incident Responders – Contextual and historic data is inaccessible in order to reduce the mean time to incident response

Security Analytics – Can't execute ad-hoc queries and large scale machine learning against enriched data for anomaly detection

Benefits

While technology advancements have expanded the threat landscape over the years creating massive cyber risk, these advancements have also opened up new cybersecurity capabilities. Cloudera's cybersecurity solution, based on Apache Spot, empowers security operations centers to reduce the mean time to incident response with complete enterprise visibility, detect advanced threats faster via machine learning, and change the economics of cybersecurity by building on an open source platform. Enterprises achieve these benefits with Cloudera through...

Unrivaled performance, scale, and analytics

Cloudera's cybersecurity solution is powered by a next generation data management and analytics platform that breaks down the traditional barriers of data ingestion, storage, processing and analysis. Enterprises can now leverage any type or volume of security data. Cloudera also extends the analytic capabilities beyond simple search and correlation allowing organizations to deploy advanced statistical and machine learning across larger volume of enriched data. This SOCs baseline normal behaviors within their enterprise across longer periods of time to more effectively detect suspicious activity.

Open data models provide complete enterprise visibility

Working with the Apache Spot community, Cloudera's solution leverages the community driven network, user, and endpoint open data models (ODM). This creates a standard schema for critical security data that is siloed across multiple applications. Accessing the open data model provides complete enterprise visibility and enriched data sets for faster investigation and advanced detection. Furthermore, storing the security data in the ODM and on Cloudera's open source platform breaks vendor lock in by disconnecting the data from the application.

Application flexibility

Buy or build applications on top of Cloudera's platform and the ODM to address new use cases while still leveraging the same enriched data set and infrastructure. With multiple Cloudera partners integrating with the ODM, SOCs can now leverage packaged visualizations and machine learning for accelerated detection, investigation, and response. If a vendor application doesn't meet the requirements, enterprises can build custom solutions using open source infrastructure and machine learning algorithms as accelerators without having to incur additional technology costs.

Community collaboration

With Cloudera's cybersecurity solution enterprises don't get a single vendor supporting them, they get an entire community. Experts in the big data, analytics, and cybersecurity community are rallying around the Apache Spot project and open data models to collectively fight back against cyber threats. With multiple SOCs adopting Apache Spot's open data models, enterprise can begin to share machine learning algorithms with one another in order to keep pace with the fast moving hacker community.

Conclusion

Using Cloudera's cybersecurity solution, based on Apache Spot, organizations can expedite threat detection, investigation, and remediation via machine learning and consolidation of all enterprise security data into a comprehensive data hub, based on open data models. Cloudera's scalability and machine learning flexibility allow security engineers to build or buy solutions that can run simultaneously on a single, shared, enriched data set and infrastructure. This helps SOCs reduce the mean time to detection and response while all working off one comprehensive view of the entire enterprise. Using the diverse open source community to accelerate shared innovations, while changing the economics of cybersecurity, allows organizations to come together to fight back against cyber threats.

cloudera.com

1-888-789-1488 or 1-650-362-0488
Cloudera, Inc. 1001 Page Mill Road, Palo Alto, CA 94304, USA

© 2017 Cloudera, Inc. All rights reserved. Cloudera and the Cloudera logo are trademarks or registered trademarks of Cloudera Inc. in the USA and other countries. All other trademarks are the property of their respective companies. Information is subject to change without notice.