cloudera®

SOLUTION BRIEF

E8 SECURITY

E8 Security

Industry

Security

Website

www.e8security.com

Company Overview

E8 Security provides a scalable, machine learning-based behavioral analytics platform to find and resolve threats that have already infiltrated the security perimeter.

Solution Overview

E8 Security's Fusion Platform is a self-learning security analytics solution that detects malicious activity hidden in the environment, prioritizes alerts based on risk, and enables security teams to rapidly respond to threats. By combining the scale of big data and the power of behavioral analytics, E8 Security's solution provides insight into the real risk and nature of security threats within the enterprise.

Solution Highlights

- Machine-learning, multi-dimensional algorithms eliminate exclusive reliance on static rules, correlations and previously known signatures
- Breaks down data silos by integrating user, network and endpoint data
- Constantly adapts to evolving threats
- Out-of-the-box integration with existing technology investments

Cloudera and E8 Security Deliver Scalable Security Analytics to Address Enterprise Cybersecurity Challenges

Identifying Unknown Threats Already Inside the Network with Machine-learning Analytics

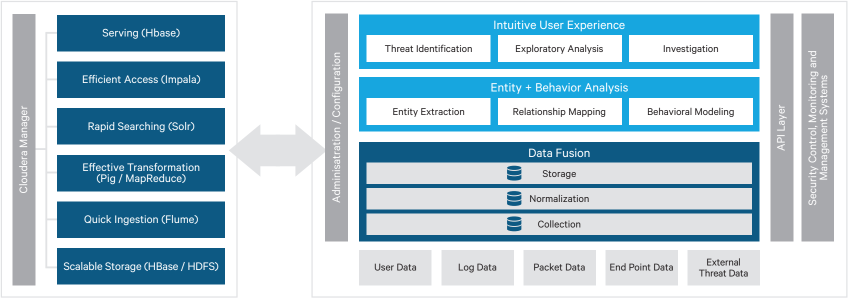
Gartner reports that the data analyzed by enterprise security organizations is doubling every year and that 40% of enterprises will be using data sets of at least 10 terabytes by 2016.[1] This data deluge is effectively burying analysts in a sea of alerts and preventing security teams from finding meaningful insights in the data, creating an "insight gap." The insight gap can be caused by

- **Reliance on manual analysis** that can't keep up with the growing volume and variety of security-relevant data
- **Failure of legacy event-monitoring systems** to provide scale and analytical flexibility to detect and prioritize threats
- **Reliance on manually configured rules and previously known signatures** that can only identify known patterns, limiting the effectiveness of legacy security tools
- Vulnerabilities created by **systems looking at data in siloes** versus across the security environment

For analysts to progress from insight to action and make smart and timely decisions requires prioritization of high-risk threats, context about threats and an understanding of their impact. The current ways analysts extract information from multiple systems and manually derive context to understand impact can cause significant delays or result in bad decisions, creating an "action gap."

Closing the Insight and Action Gaps

E8 Security applies machine learning and multi-dimensional modeling that examines user and device behaviors to identify anomalous activities. Machine-learning models automatically learn behaviors and relationships and identify attacker activities within the enterprise. Advanced threat models expose threat activities such as command and control (C2) communications, lateral movement, credential compromise and established attacker persistence. These sophisticated analytics enable machines and humans to optimize their threat identification abilities and gain insight into the real risk and nature of security threats within the business environment—closing both insight and action gaps.



[1] MacDonald, N. Information Security Is Becoming a Big Data Analytics Problem. March 2012.

Benefits of Cloudera

Stores and Analyzes Any Type of Data

- Leverage the full power of your data to achieve pervasive analytics, increase business visibility, and reduce costs
- Bring diverse users and application workloads to a single, unified pool of data on common infrastructure; no data movement required

Enterprise Approach

- Compliance-ready perimeter security, authentication, granular authorization, and data protection through encryption and key management
- Enterprise-grade data auditing, data lineage, and data discovery

Industry-Leading Management and Support

- Best-in-class holistic interface that provides end-to-end system management and zero-downtime rolling upgrades
- Open platform ensures easy integration with existing systems
- Open source to achieve stability, continuous innovation, and portability

Benefits of E8 Security

- Detect previously unknown persistent threats that legacy systems can't find
- Automatically provide a risk-prioritized view of threats based on behavioral anomalies and context
- Investigate and validate insights to rapidly respond to threats
- Improve the effectiveness of existing security infrastructure

Built on Cloudera Enterprise

At the core of E8 Security's effectiveness is the solution's ability to automate manual analysis, process large volumes of security data sets that are often unstructured or semi-structured, and consolidate and centralize previously siloed data. E8 Security's solution rapidly accesses the underlying data, analyzes it and manages the diverse analytics needs of enterprise security operations.

To enable these capabilities, E8 Security's Fusion Platform is built on Cloudera Enterprise. Cloudera Enterprise is designed specifically for mission-critical environments and addresses the needs of enterprise security by delivering advanced system management tools, dedicated support and community advocacy.

For E8 Security, Cloudera Enterprise provides:

- A flexible and scalable SQL interface via Cloudera Impala for fast access and analytics
- Apache Spark for optimized data processing and high performance in-memory compute for real-time analytics provided by E8 Security's solution
- The ability to allow users to run SQL workloads, a programming environment users are already familiar with, to deliver analytics capabilities with massively parallel processing (MPP) and ANSI SQL
- Rapid deployment, easy configuration and efficient operation with Cloudera Manager, a centralized console for monitoring and reporting

About E8 Security

E8 Security is transforming security operations by automating the learning of user and device behaviors to discover malicious activity unknown to security analysts, resulting in improved alert quality and accelerated investigations to make security operations more proactive. E8 Security raises the bar, as the first behavioral analytics vendor to make it easier for security teams to quickly identify unknown threat behaviors across endpoints, users and networks. The E8 Security Fusion platform provides a focused view of the network, so that analysts can quickly see hidden threats and know where to spend their time, reducing the investigation time from hours to minutes. In short, E8 Security helps security teams to detect, hunt, and respond by recognizing what is normal in their network so they can quickly respond to what is not. E8 Security is headquartered in Silicon Valley and is funded by Strategic Cyber Ventures, March Capital Partners, Allegis Capital and The Hive. Find out more at www.e8security.com.

About Cloudera

Cloudera delivers the modern platform for data management and analytics. The world's leading organizations trust Cloudera to help solve their most challenging business problems with Cloudera Enterprise, the fastest, easiest, and most secure data platform built on Apache Hadoop. Our customers can efficiently capture, store, process, and analyze vast amounts of data, empowering them to use advanced analytics to drive business decisions quickly, flexibly, and at lower cost than has been possible before. To ensure our customers are successful, we offer comprehensive support, training, and professional services.
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