SOLUTION BRIEF

Digital Bank of the Future
Financial Services

Reduce Money Laundering Risks with Rapid, Predictive Insights

Financial institutions face new challenges in preventing fraud and theft directed at them and their clients

Executive Summary

Money laundering is the process by which the illegal origin of wealth is disguised to avoid suspicion and to wipe the trail of incriminating evidence.

In response to the growth in money laundering and terrorist financing activities worldwide, regulators have stepped up compliance mandates. As a result, financial institutions have experienced dramatic increases in fines for regulatory violations imposed by a growing array of authorities. In 2012, the US Office of the Comptroller of the Currency (OCC) began applying its Supervisory Guidance on Model Risk Management (OCC 2011-12) to Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) compliance practices. Since then, financial institutions have increased their adoption of more rigorous analytics use to improve their BSA/AML monitoring and Know-Your-Customer (KYC) programs.

With the rise of online and mobile transactions, financial institutions face new challenges in preventing fraud and theft directed at them and their clients. It is imperative for these organizations to find new ways to optimize AML transaction monitoring processes. The problem is that criminal organizations are using increasingly sophisticated and hard-to–detect approaches, and they are getting more effective at obscuring their activities behind the growing complexity of the global financial infrastructure.

Why Current AML Compliance Programs Are Failing

It is no longer enough to use standard technologies and controls and accept any undetected money laundering as part of doing business. Rather, regulators require firms to be more proactive, innovative and thorough by using big data analytics, machine learning and visualizations to uncover new and emerging risks. These technologies make it easier to pinpoint risk indicators that may not have been visible before. They also eliminate guesswork and enable earlier detection.

But progress toward meeting these requirements is being hindered by a number of challenges. First, data is typically scattered across multiple systems. Financial institutions have long struggled with data silos created by multiple legacy systems, data warehouses and best-of-breed packaged application systems. This causes data inconsistencies, integration difficulties and increased maintenance costs. With multiple repositories of data, there is also no single source of truth readily available for data exploration and analysis. Additionally, traditional AML tools provide limited flexibility in analyzing and correlating petabytes of data across financial instruments, lines of business, regions, transaction types and omnichannel touch points. These tools are also not designed to ingest and correlate data from new data sources such as mobile.

They generate high volumes of low value alerts. Changing red flag detection scenarios to meet stringent risk thresholds is often a time-consuming process that needs valuable resources to get the job done. By the time anomalies indicating emerging risks are detected, damage has already been done.

The Path Forward: AML Requires an Enterprise Data Hub and Advanced Analytics for Big Data

So, where do financial institutions start? First, they will need an up-to-date, complete and single version of data for all analysis and reporting. When they have a trusted, single source of data, they can run analyses quickly and confidently. The ability to rapidly analyze large volumes of both structured and unstructured data that comes from a wide variety of sources demands a technology platform that is specifically built for and dedicated to that purpose. It requires a high-performance platform that can ingest billions of data records (representing petabytes and terabytes of data), perform advanced analytics and deliver results in real time or minutes versus days and weeks. It requires consolidated data management.

The introduction of an enterprise data hub (EDH) built on an open-standard and open-source Apache* Hadoop* framework provides a cost-effective way for financial institutions of all types and sizes to aggregate and store all their data, in any format, for all types of workloads, in a highly secure environment. For the first time, compliance teams and data scientists can access rich data sources, blend and analyze data from any source, in any amount, detect money laundering patterns across omnichannel touch points, financial instruments and asset classes, model risk and gain valuable real-time insights that deliver results.

By aggregating, analyzing and correlating petabytes and terabytes of internal and external data of all types in a single platform, financial institutions can solve some of the toughest problems around money laundering, fraud, data and regulatory non-compliance breaches that are costing them billions in losses annually.

In addition, financial institutions will need powerful analytical and data visualization capabilities to enable proactive, unstructured searches that can detect potential anomalies before they are uncovered by internal audit or third parties. By leveraging an EDH and high performance analytics, financial organizations can:

- **Scale the surfing and analysis of big data to efficiently detect known, unknown and emerging risks.**
  Firms must be more proactive and use unstructured searches of big data and data visualizations to scan large amounts of data. Graphs, decision trees, geospatial and other methods make it much easier to identify patterns or relationships that seem irregular or suspicious.

- **Quickly drill down into related information and determine if a given anomaly is truly a risk.**
  Further analyses can be performed to determine the extent of the risk and if it represents a new risk typology that must be put into production using automated AML scenarios.

- **Generate accurate reports of new and emerging risks for regulators and executives, quickly and efficiently, even as requirements change.**
  Regulatory reporting requirements are always a moving target, so firms need flexible reporting solutions. And executives need reports that visualize findings so they can quickly grasp what the data means and enable them to assess macro-level trends that are happening within their firm, such as large spikes in product use and the international flow of funds.

- **Perform ad hoc analyses in real-time to address questions and issues that arise.**
  Decision makers and third parties simply don't have time to wait until the next meeting to get answers. They need - and increasingly expect - answers immediately so they can take action to mitigate risks. Using in-memory technology and data visualization software allows users to scan large amounts of data through graphs, decision trees and other methods to identify data points or correlations that seem suspicious.

The SAS and Cloudera Advantage for AML

SAS and Cloudera provide a comprehensive infrastructure, solutions, and services to tackle AML holistically. Combined, they can:

Improve data access and data preparation for analytics
Cloudera Enterprise powered by Hadoop is a single platform that can serve as a landing place for consolidating and analyzing all data, in any format, from any source for all types of workloads – all in a highly secure environment. Unlike "rip-and-replace" options, Cloudera Enterprise is designed to augment the capabilities of existing AML and storage solutions. With Cloudera, financial institutions can aggregate, blend, analyze and correlate petabytes of data from any source cost-effectively. Moreover, only Cloudera provides comprehensive, compliance-ready data security and governance throughout the Hadoop cluster, a critical component for financial institutions working with sensitive and personal information.

Reduce data movement and replication
This means less time is spent on data preparation and more time on using analytics to drive faster and better decisions. Simplified data preparation saves IT resources and moves the data quality functions into the hands of those who understand the data better. Intuitive web-based user interfaces reduce

Hadoop skills gaps and shorten the learning curve. Users can easily create custom data directives (e.g. filters, aggregations and data movement commands) and reuse them when needed. Data can be batch loaded or streamed real-time through Spark – a key component of Cloudera Enterprise.

Deliver faster, analytics-based decisions
The speed of the SAS Analytics* and SAS Anti-Money Laundering* solution is accelerated when running on Cloudera Enterprise by spreading the processing across the nodes in the cluster. In-memory analytics allow you to load data into memory once, then focus on segmenting your data and building multiple models to target groups simultaneously. A guided selection of analytic techniques speeds exploration and insights while reducing latencies often associated with model development. Automatically deploy analytical models into Hadoop and score new data using SAS directly within each node of a Hadoop cluster for fast and efficient processing without data movement.

Easily combine data exploration with predictive modeling
Financial institutions can discover and evaluate new opportunities for every possible angle. Cloudera Enterprise includes a variety of query frameworks - including Impala*, the fastest interactive SQL database on Hadoop – for rapid data discovery. Combined with SAS In-Memory Analytics*, it allows more scenarios and iterations to be run to produce more precise insights. Modelers can quickly test new ideas, try different modeling techniques and refine models on the fly to produce the best results – using data volumes never before possible. Proven, built-for-purpose statistical algorithms and machine-learning techniques deliver precise answers quickly and confidently.

SAS® Anti-Money Laundering

SAS Anti-Money Laundering takes full advantage of high-performance analytics capabilities to provide the most accurate, complete solution for detecting, investigating and reporting on potential illicit activity – including customer due diligence, suspicious activity monitoring, watch-list filtering, Financial

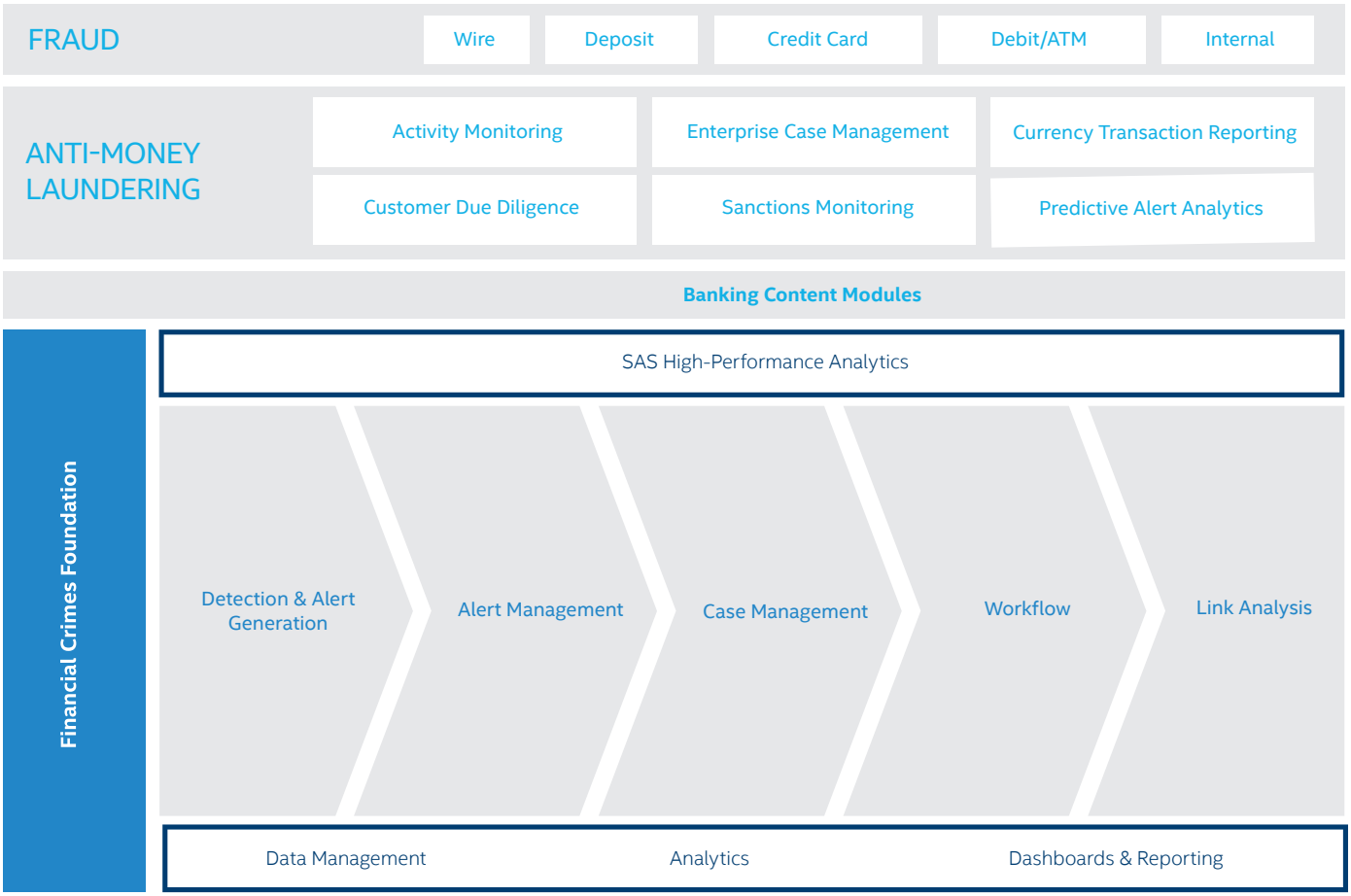

Figure 1. SAS Financial Crimes Suite, including Anti-Money Laundering.

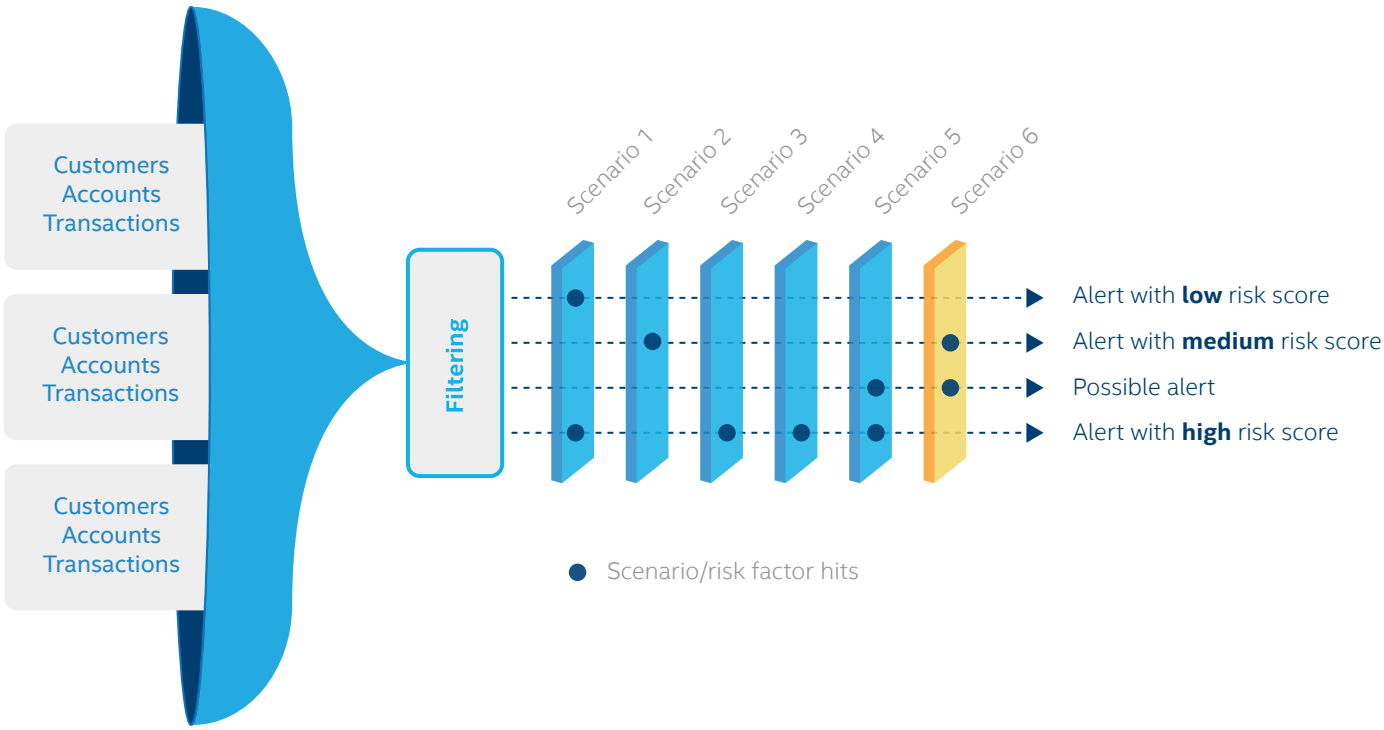

Figure 2. Risk factor and alert generation process.

Crimes Enforcement Network (FinCEN) e-filing support and case management. Through enhanced scenario tuning and what-if analysis, SAS Anti-Money Laundering dramatically reduces from hours to minutes the time it takes to provide investigators the relevant information, conduct preliminary analyses and identify areas that need further attention, such as suspicious transactions or unusual patterns. This creates more time to focus on the most critical cases.

Leveraging analytics helps increase both the depth and breadth of transaction monitoring for illicit activity. High-performance analytics and multiple detection methods monitor more risks—in very large data volumes—in less time which allows investigative resources to be reallocated to other emerging risks. This is done in a user interface with a drag–and-drop approach that does not require any coding. In order to build a better picture of customer interactions , SAS uses multiple data sources across departments and additional databases. The solution provides a flexible workflow environment that ensures standard processes are adhered to in order to meet internal policy requirements, as well as compliance standards set by the relevant regulatory agency. With an expedient process to copy scenarios, organizations can more rapidly adjust for segmentation and threshold tuning. And they can visualize data with dashboards. For triage, distribution and reporting, the investigative case management module is fully auditable and tracks all aspects of the investigation. And with an automated workflow, organizations gain greater control of case management for multiple workgroups.

Part of the SAS Financial Crimes Suite* (figure 1), the SAS AML solution provides landing specifications for how a system accepts multiple data source systems, including demographic, and third party data. Packaged data management prepares data for monitoring, and the data model is optimized for AML analysis. Alerts are generated and populated into a Knowledge Center schema, and stored in the client's database of choice. Risk scenarios can be status-based or behavior based, and risk factors will be generated for each alert (figure 2). Advanced algorithms are used to identify all accounts with similar transactional behavior to a targeted suspicious account. A visualization tool then displays accounts which are linked to those of alert interest, while routing rules and suppression rules are used to eliminate redundant alerts.

During the Alert Analytic process, analytical models are applied to all alerts generated by the system (figure 3). The SAS AML solution provides templates that are presented to all models, which may contain a set of risk variables. Alerts are scored, and high-scoring alerts are triaged for investigation.

An Investigation User Interface manages and disposes of alerts. Query functionality allows an end user to view information on alerts, accounts, customers and watch lists. Case Packaging allows multiple alerts to be packaged as a single alert. Actions

and disposition codes are captured for review and audit purposes, and the interface supports comments, attachments and automated regulatory filing.

- **Data management.** Comprehensive capabilities, including a banking-specific data model, provide access to cross-channel data via an easy-to-use, intuitive interface. In addition SAS provides an intuitive user interface. Data analysts can run SAS code on Hadoop for even better performance. Access and load Hadoop data fast. Turn big data into valuable data with quick, easy access to Hadoop and the ability to load to and from relational data sources as well as SAS datasets. With Entity Link Analysis, organizations can visualize demographic case file relationships to understand the source of funds and connections between suspicious customers that may indicate rings on the client site. Peer group anomaly detection compares a customer's behavior to their previous historical behavior and to the behavior of their peer groups (e.g. comparing a convenience store to other convenience stores' financial transactions within a similar geography).

- **Suspicious activity monitoring and reporting.** A robust, flexible scenario engine automates transaction monitoring and behavior detection for Suspicious Activity Report (SAR) and Currency Transaction Reporting (CTR) filing.

- **Investigation, alert management, routing, and triage..** A web-based investigation interface provides access to a knowledge center database, which serves as the system of record for regulatory and auditing purposes. Predictive analytics significantly reduces false positives, cuts staffing hours required for triage and reduces alerts worked by personnel.

- **AML optimization.** Predictive models score the likelihood that an alert will contribute to a productive investigation. SAS Transaction Monitoring Optimization lets analysts use in-memory architecture to test AML models against large data volumes. The technology also integrates industry-vetted methodology for segmentation, validation, tuning and simulation of AML models.

- **Customer due diligence/KYC risk scoring and classification.** Customers' on-board risk scores are automatically integrated with actual transactional behavior, and risk classifications can be reassessed as needed.

- **Watch-list matching.** Sanctions and other watch lists can be imported to identify persons, organizations or high-risk jurisdictions that represent regulatory risk.

- **Integrated case management**, an easy-to-use, web-based user interface supports the management, investigation and reporting needs of analysts and investigators.

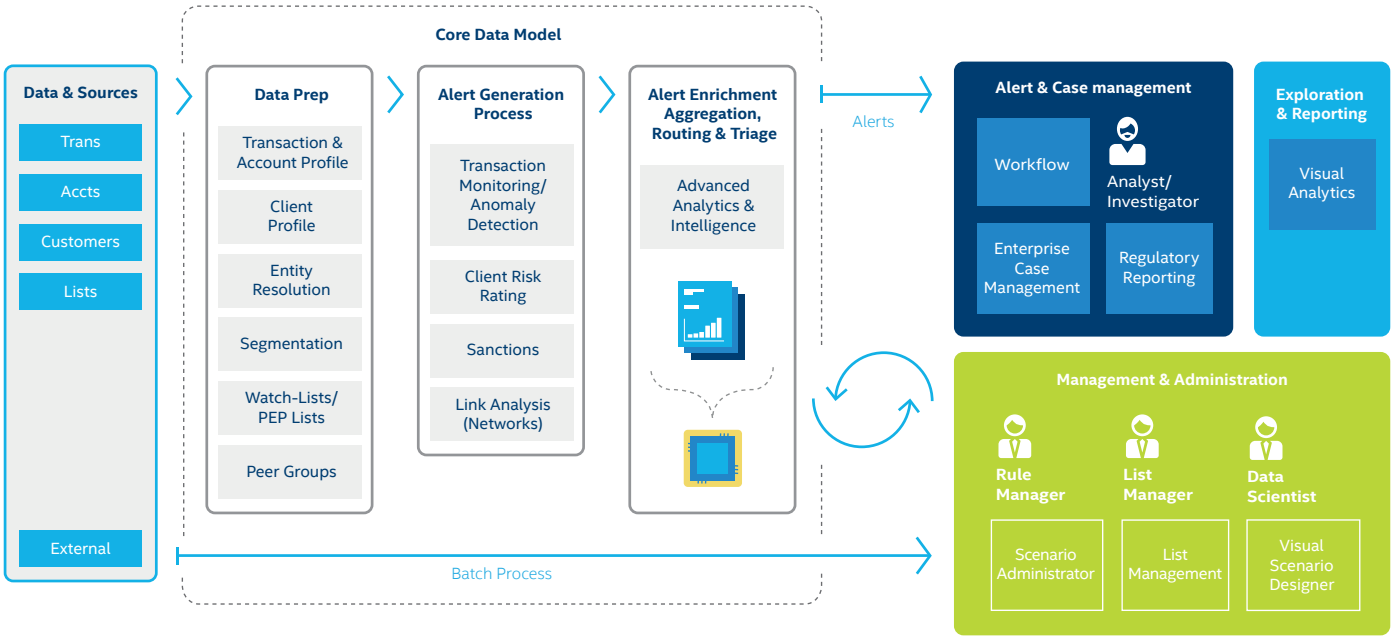

Figure 3. Data collection, processing and analysis framework.

Cloudera's Enterprise Data Hub

An EDH at the core of the information architecture promotes the centralization of all data, in all formats, available to all business users, with full fidelity and security. The Cloudera Enterprise data hub offering (figure 4), built on Apache Hadoop is the ideal platform for AML because it augments all of the core functions of a specialized system to better handle big data: data collection, data preparation, automated evaluation, model building, and investigation. The modern AML architecture is fully integrated with an enterprise data hub, with Hadoop initially staging massive complex data for legacy solutions to provide runtimes for the predictive models and detect fraud. Beyond the introductory use case of more expansive and affordable storage, Hadoop's natural fit for back-testing against long-term descriptive data is gaining popularity for more advanced AML workloads, as is the use of other components in the Hadoop stack for exploration, discovery, investigation, and forensics.

Moreover, new cyber-surveillance applications have led to billions of dollars in loss avoidance for the financial services industry. As a result, these systems must be enriched with much larger and more diverse data sets to isolate signals of possible money laundering. With Cloudera Enterprise, financial institutions can aggregate, analyze and correlate data from existing and new vectors of threat to more effectively detect patterns and prevent complex money laundering schemes.

Spark - a key component of Cloudera Enterprise data hub (figure 5) - for machine learning and event stream processing, enables financial institutions to aggregate and analyze massive amounts of data from multiple sources including web, geo-location, electronic communications, enterprise applications and trading systems to detect patterns and identify fraudulent activities. With Spark, financial institutions can perform real-time queries, quickly model and execute complex data flows and accelerate the repetitive processing required by iterative algorithms.

Cloudera Enterprise, with Apache Hadoop at the core, is:

- **Unified** – an integrated platform, bringing diverse users and application workloads to one pool of data on common infrastructure, no data movement required.
- **Secure** – compliance-ready perimeter security, authentication, granular authorization and data protection (through encryption and key management).
- **Governed** – enterprise-grade data auditing, data lineage and data discovery.
- **Managed** – best-in-class holistic interface that provides end-to-end system management and key enterprise features, such as zero-downtime rolling upgrades.

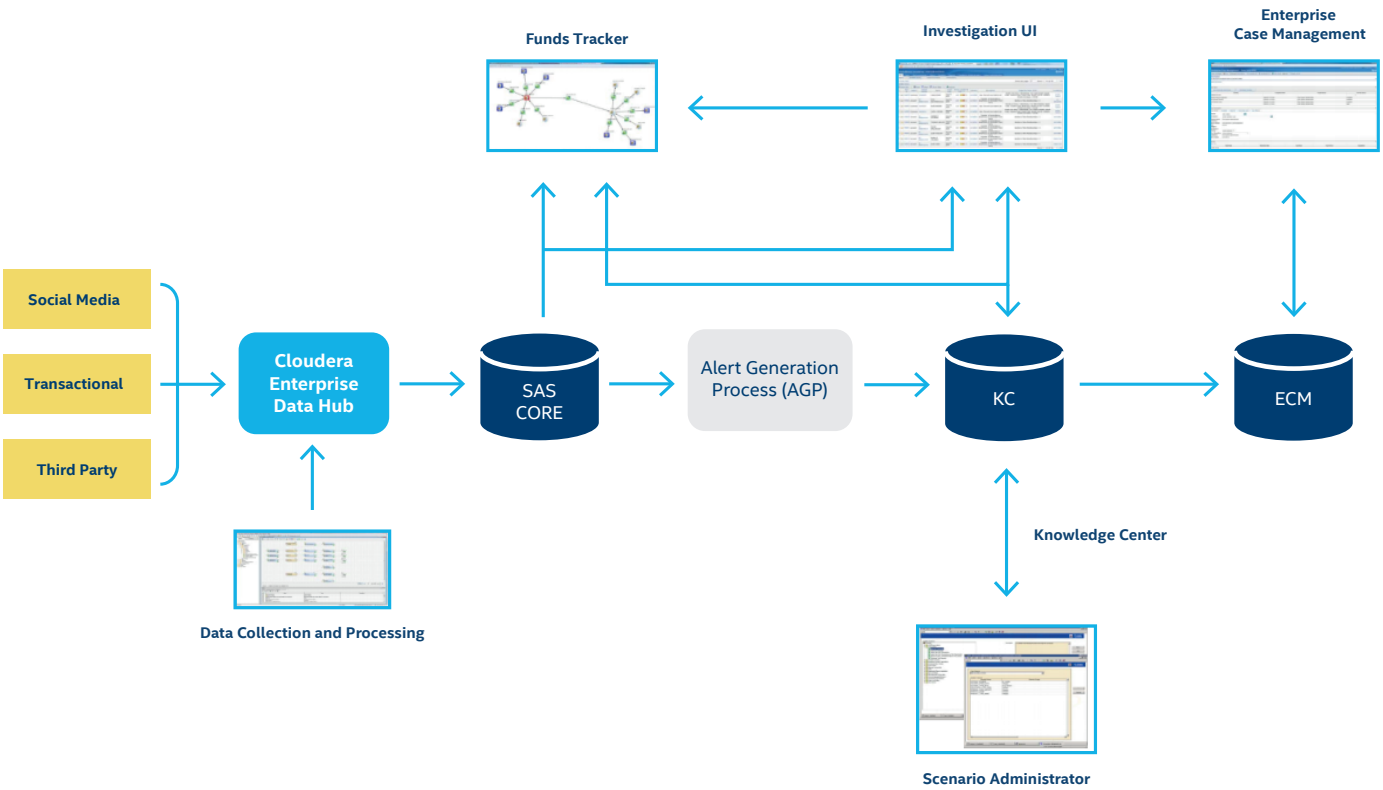

Figure 4. Integrated Cloudera Enterprise Data Hub and SAS AML solution.

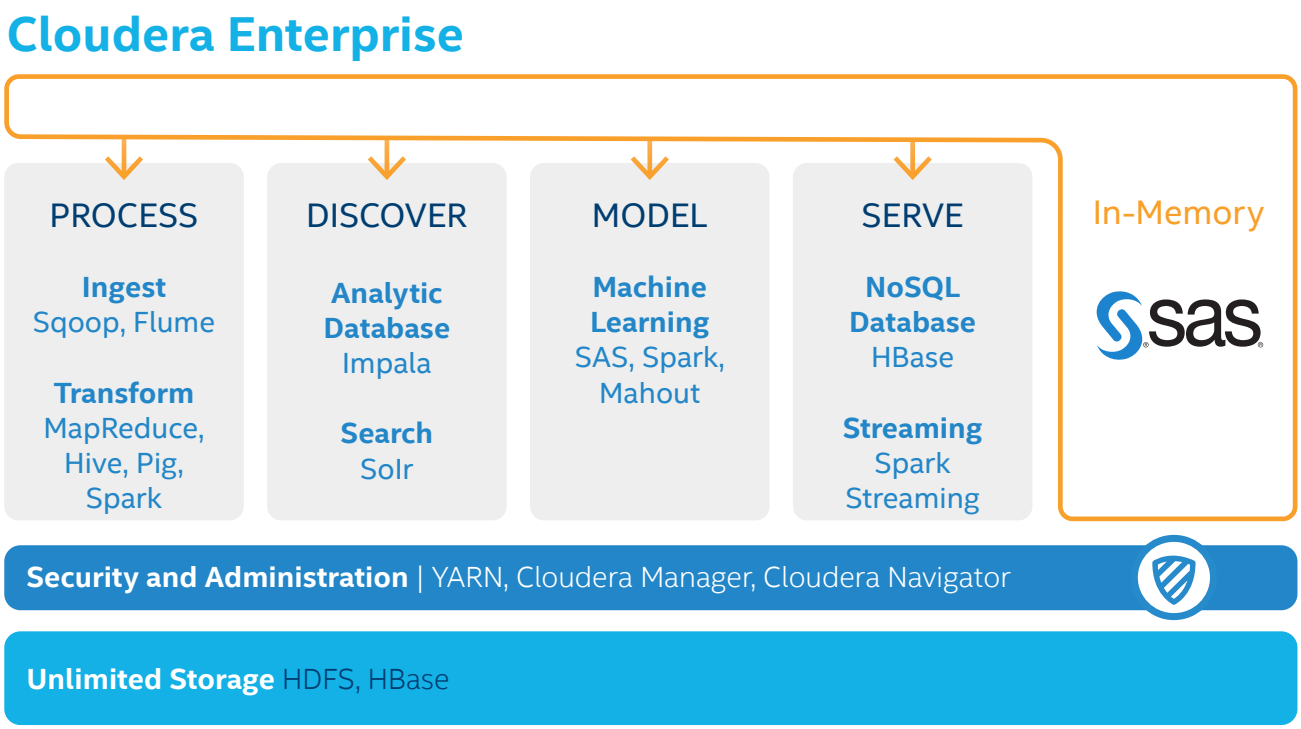

Figure 5. Integrated SAS and Cloudera solution framework.

- **Open** – open platform means both open-source and open-standard so organizations can be confident that their investment in Hadoop will be sustainable, portable, better integrated with the ecosystem and of the highest quality.

The Cloudera Enterprise data hub solution offers security, flexibility, scalability, and affordability and is extending existing and new investments in dedicated fraud-detection platforms like SAS AML solution by increasing the volume, age, and variety of data that can be examined while speeding up data transformation for faster time to insight. Once such massive data is consolidated, Hadoop can increasingly take on more advanced AML workloads such as entity matching — the process by which records from disparate systems are mapped to individuals or legal identities — while associated tools in the data hub like Cloudera Search* and Impala* remove the complexity of model development, process automation, and case investigation.

A Reliable, Scalable and High Performance Infrastructure

SAS applications provide an integrated environment to solve a variety of complex business problems, so it is no surprise that they require strong computing performance, scalability and reliability. Fortunately, they get all that and more with platforms using the Intel® Xeon® processor E5 family for distributed computing environment and Intel® Xeon® processor E7 v3 family and Intel® Solid State Drives (Intel® SSD) with Non-volatile Memory Express (NVMe) for complex and real-time analytics operation.

The Intel Xeon processor E7-4400/8800 v3 product families' key gains over previous-generation technology include:

- **Higher core count.** Use fewer servers for the same work with 72 cores per 4 socket server.
- **Increased memory capacity and I/O.** Up to 6 TB per 4-socket server and 12 TB per 8-socket server
- **Highly reliable.** Count on world-class uptime with a platform designed for five nines (99.999 percent) reliability.[1]

These advantages provide financial institutions with powerful weapons in their ongoing battle against fraud, such as:

- **Applying business context** for optimizing models and detecting emerging risk exposures.
- **Better analytics** to reduce false positives and better manage human costs
- **Faster time-to-detection**, using high-performance analytics for more timely scenario tuning
- **Strengthened model governance**, for easier modifications and faster response to changing fraud schemes

The Power Behind Strong Analytics

SAS is the leader in analytics. Through innovative analytics, business intelligence and data management software and services, SAS helps customers at more than 83,000 sites make better decisions faster. Since 1976, SAS has been giving customers around the world THE POWER TO KNOW®.

Cloudera is revolutionizing enterprise data management by offering the first unified platform for big data, an enterprise data hub built on Apache Hadoop. Cloudera offers enterprises one place to store, access, process, secure, and analyze all their data, empowering them to extend the value of existing investments while enabling fundamental new ways to derive value from their data. Cloudera's open source big data platform is the most widely adopted in the world, and Cloudera is the most prolific contributor to the open source Hadoop ecosystem. As the leading educator of Hadoop professionals, Cloudera has trained over 40,000 individuals worldwide. Over 1,700 partners and a seasoned professional services team help deliver greater time to value. Finally, only Cloudera provides proactive and predictive support to run an enterprise data hub with confidence. Leading organizations in every industry plus top public sector organizations globally run Cloudera in production.

Intel (NASDAQ: INTC) is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices. Additional information about Intel is available at intel.com.

To learn more about SAS Anti-Money Laundering, Cloudera Enterprise Data Hub and Intel, contact your SAS, Cloudera or Intel representative or visit **www.sas.com**, **www.cloudera.com**, **www.intel.com**.

[1] Source: **http://www.intel.com/content/dam/www/public/us/en/documents/brochures/sas-intel-solution-for-enterprise-analytics.pdf**

1016/JW/CAT/PDF ♻ Please Recycle 108829_51362.0417 335157-001US