unifi

Minimize Your Risk with the Unifi Compliance Data Hub

Compliance Data Hub

Manage financial compliance more efficiently

Adapt quickly to regulatory requirements like GDPR

Detect fraud and suspicious activity sooner

Overview

The regulatory environment for financial institutions is constantly changing. Strict government regulations are enforced to ensure the financial stability of the U.S., even the global economy. U.S. based financial service providers must comply with regulations and implement processes to prevent fraud and other illegal activities or risk steep fines.
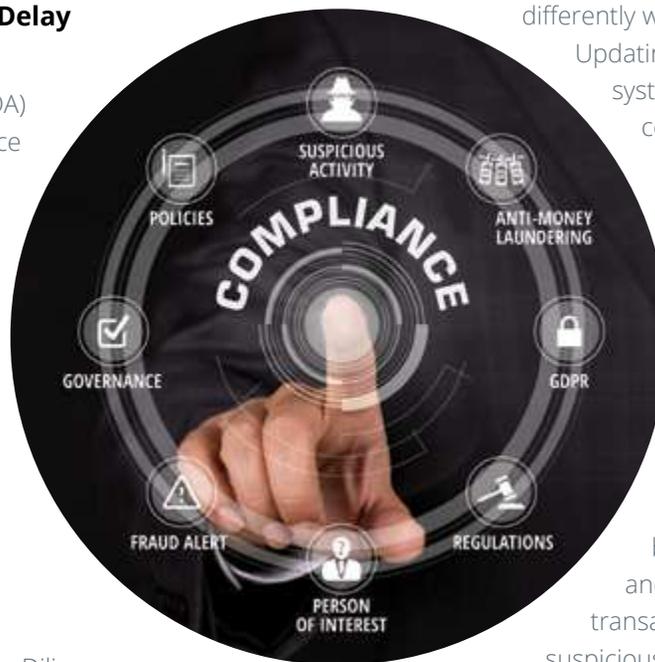
The nature of financial institutions and how their businesses have grown—often through acquisition--usually results in numerous data silos. One peer-to-peer money transfer company has amassed over 1200 data sets. This exacerbates the function for compliance analysts, who must be able to readily access any and all data as it pertains to financial compliance.

Fragmented Data Causes Delay in Compliance Insights

Compliance Data Analytics (CDA) teams support all of compliance requirements for bulk data extraction, analysis, business optimization and modeling. CDA teams are often responsible for providing support across the organization including departmental groups in Financial Intelligence, Program Office, Risk Mitigation, Global Back Office, Transaction Monitoring & Reporting, Advanced Risk & Regulatory Projects, Global Due Diligence in addition to corporate finance and product development and management.

As the organization grows the number of inbound requests for insights grows exponentially. Responding to requests for data insights from across the organization is often takes days and sometimes weeks. Simply hiring more compliance analysts does not solve the problem, as one financial institution learned having grown their CDA team from 70 to over 400 analysts.

The problem lies in the distributed and siloed data. Without master data management and governance different teams end up deriving values and calculations differently which compounds the problem. Updating a data warehouse from core systems at different cadences also complicates analysis and uses substantial IT resources.

A Unified View of Consumer Transactions

Without a unified view of transactions, behavioral modeling becomes very challenging. To detect Fraud and Anti-Money Laundering (AML), CDA teams must be able to track consumers and agents across platforms, transactional anomalies, and other suspicious activities. For example, CDA teams have a responsibility for tracking and identifying multiple transactions from the same account that fall below the $10,000 transfer notification value but add up to suspicious amounts. Understanding the transactional relationship between the consumer and agent requires enhanced due diligence and Risk Ranking of consumer behavior. This is a Data Protection Act requirement and must be addressed or the institution risks severe fines.

When the Government Comes Knocking

Under the United States Banking Anti-Terrorism law, the government can request information from any U.S. banking institution related to the movement of funds

Unifi Compliance Hub Reference Architecture
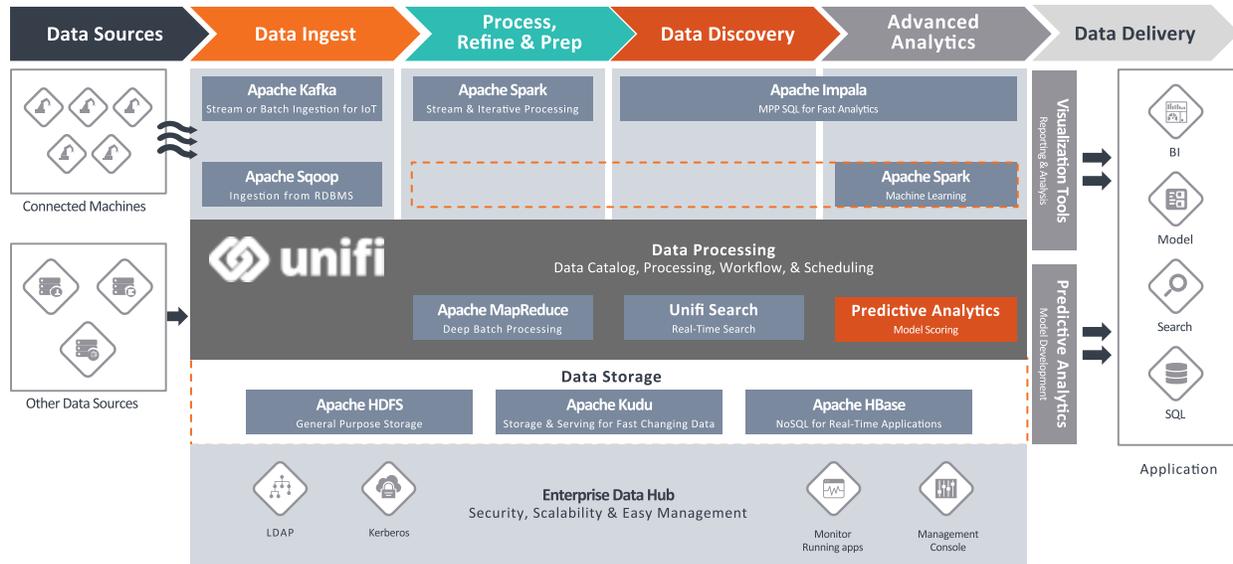
into or out of the U.S. banking system. The Department of Justice may issue a subpoena for transaction information, the Department of Homeland Security can issues a subpoena based on a person of interest etc. Responding to these information request in a timely fashion is critical to avoid fines and fall under closer operational government scrutiny.

Geographically dispersed, separate data silos exacerbates the problem of timely response to this type of request. One peer to peer money transfer organization would outsource such requests to a professional services provider whose response time was measured in weeks, and whose bill for services approached six figures for each request.

Deploy the Unifi Compliance Data Hub

The answer to the compliance reporting and analytics challenge is to consolidate all data sources and provision a self-service reporting, IT-governed, data environment across the business. This provides analysts and business users the ability to search across all data, select data sources of interest and then run a series of pre-defined data jobs to gain insights quickly. Ad hoc analytics is also dramatically improved by the inclusion of AI-assisted data cleansing, normalizing, enrichment, transformation, filtering and formatting.

Data Governance: The Unifi data governance capabilities provides the tools to maintain IT control over the compliance data. The Unified data environment provides a single source of truth for data and the community features of the product allows users to interact, rate, and add commentary to data sets. This provides consistency of insights across data sets and overall, improves the confidence in the data being used for analysis.

Time to Value: The ability to view new sources in hours as opposed to months provides a significant ROI. For example, with the Unifi product, the analyst can enter the name of a person of interest into the Unifi search and receive transaction data from all sources within the organization in minutes. No longer is the analyst required to make a request for the data that takes weeks or more to receive. Integrating new data sources and combine them with existing compliance data allows for more accurate predictive modelling and fraud prevention.

Scalability: Rather than create ETL functions for a few, specific compliance tasks, the Unifi Compliance Data Hub address every compliance requirement equally. This alleviates IT support for compliance analytics tasks and dramatically improves response times across the business.

GDPR Compliance – The Clock is Ticking

The European Union General Data Protection Regulation comes into effect in May, 2018. Publically expounded as a consumer bill of rights, it aims to offer EU citizens some control and reassurance over their personally identifiable information. The legislation requires any organization who stores EU consumer Personally Identifiable Information (PII) to store this data securely, to notify the consumer if there is a data breach, allow the consumer to move their data from one service to another for example, in the case of a mobile phone carrier, enable the consumer to delete their information from records including search results, and to restrict the processing of their personal data except under certain conditions such as medical treatment, vital interests etc.

Analyst

Data Steward

RegAlert! Real-time Monitoring and Governance

The Unifi Compliance Data Hub is ideally suited to provide protection for GDPR compliance. The RegAlert! monitoring features of Unifi prevents unauthorized users from accessing GDPR data based on a policy engine and notifies the data steward. The comprehensive governance features of the platform provides row and column level security for any data set. So analysts and other users can be granted restricted access to the data. That is, they can use the data to run analysis without seeing the actual values. In addition to source data, Unifi discovers and monitors derived data sets with sophisticated data lineage capabilities. Derived data sets are the most likely cause of future, expensive compliance infractions.

Future Proof Your Compliance

Constantly changing regulatory compliance requirements adds complexing to the day-to-day operations of every financial institution. The centralized, Unifi Compliance Data Hub allows the organization to adapt quickly to the regulatory landscape and to maintain operation efficiency across the organization.

Unifi governance features provide row and column level security so analysts can use the data for visualizations without violating compliance policies.

About Unifi Unifi provides Data as a Service in an integrated suite of self-service data tools that include Governance & Security, Cataloging & Discovery, AI-Assisted Data Preparation, Community Collaboration and is Cloud-Optimized. Governed by IT and operated by business users, Unifi alleviates data bottlenecks and delivers faster business insights.