Palantir Foundry for Anti-Financial Crime 360

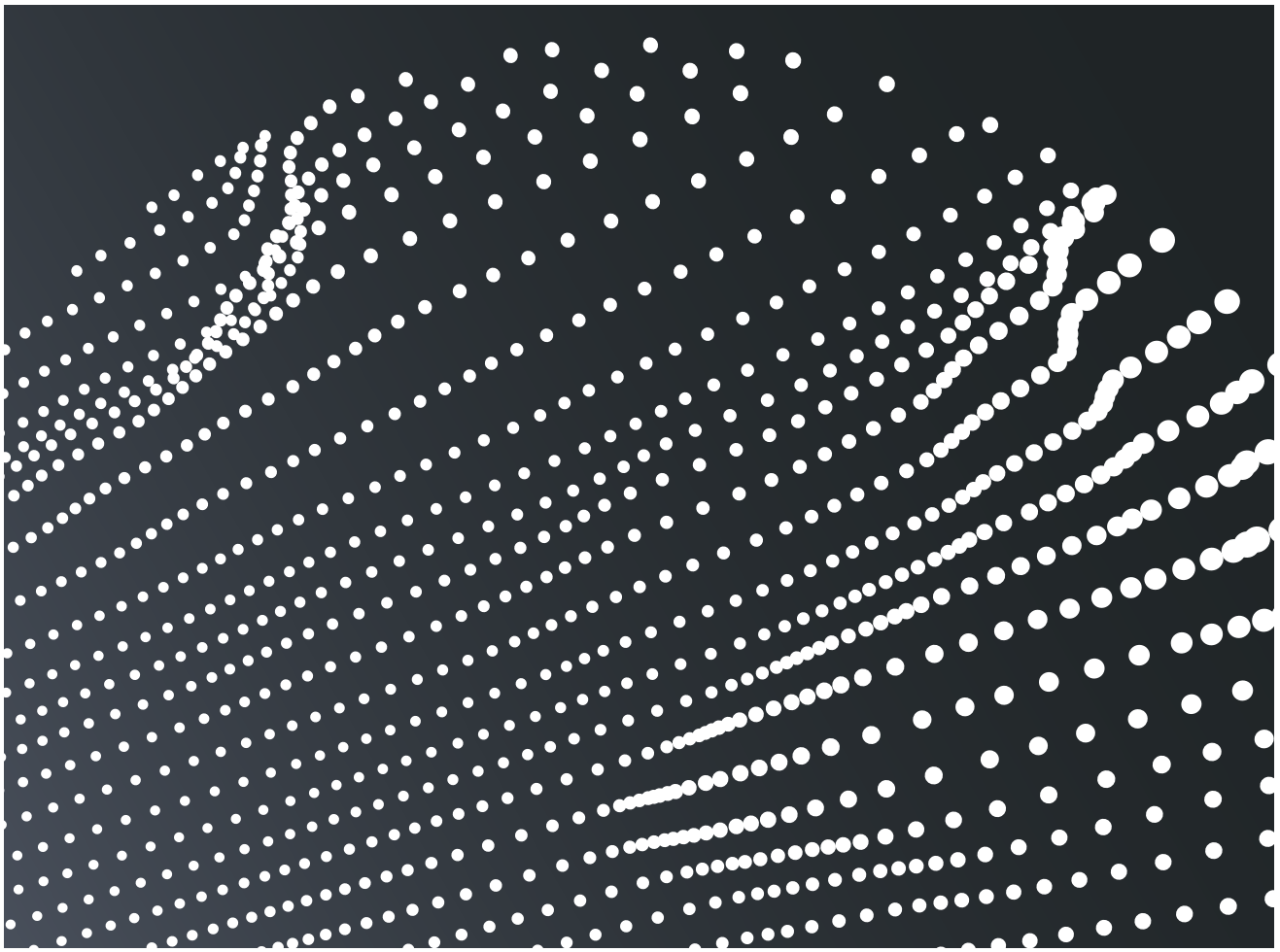
Palantir

SOLUTION OVERVIEW
– WHITEPAPER

PALANTIR
TECHNOLOGIES

PALANTIR.COM

COPYRIGHT © 2022



Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

Introduction

The 2016 Panama Papers leak saw the unsavory dealings of politicians, businesspeople, oligarchs, and the like splashed across front pages around the world. In the immediate aftermath of the revelations, public outrage sparked protests, forced high-profile politicians to resign, and spurred innumerable investigations. Beyond its near-term effects, however, the Panama Papers scandal marked a seismic shift: it ushered in a new era of unprecedented scrutiny on financial crime, with financial institutions under the microscope.

As scrutiny has increased, so too have the repercussions of missteps. Financial institutions face damaging operational, financial, reputational, and regulatory consequences for violations, from enormous fines to shuttered business lines. In the aftermath of a breach, they may see their revenues impacted by a barrage of negative publicity even as they incur massive legal costs. With the proliferation of senior manager and executive accountability regimes in many jurisdictions, even individuals increasingly face financial penalties and administrative sanctions for compliance failures.

At the same time, the anti-financial crime landscape has only grown more complex. Financial institutions must translate complex regulations and frameworks into action across millions of clients with labyrinthine networks that span the globe, making split-second decisions in the face of intense regulatory scrutiny. While many institutions have adopted new technologies, developed robust policies and procedures, and deployed large compliance teams, most lack the connective tissue to unify these component parts.

This informational and functional isolation leaves financial institutions with a dangerously windowed perspective. Without the ability to connect disparate anti-financial crime processes, they make crucial decisions in silos, and the potential for missed signals skyrockets. This not only increases the probability of damaging impacts, but also hampers financial institutions' ability to streamline operations and gain efficiency over time.

To improve risk posture and prepare for future regulatory and institutional needs, financial institutions require solutions that can provide end-to-end customer visibility and operate flexibly, fitting into existing architecture and adapting to ever-evolving demands.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

Challenges

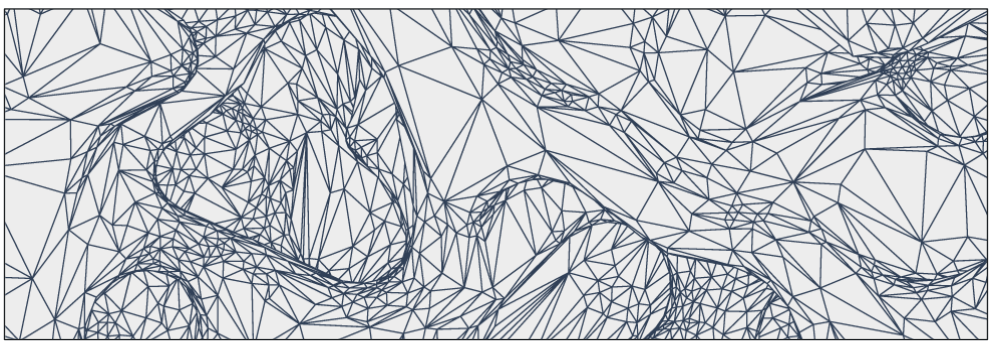
Financial institutions face a slew of obstacles in designing and implementing integrated anti-financial crime programs, as well as generating — not to mention operationalizing — a holistic view of risk exposure.

01 Decentralized View →

Often constrained by siloed systems, many financial institutions struggle to maintain an accurate, all-encompassing view of their clients and anti-financial crime operations more broadly. This windowed perspective leaves them vulnerable to missed indicators, undetected patterns, bad actors, and more, increasing the risk of regulatory failures and reputational damage.

The complexity involved in managing a relationship with a large corporate entity such as a multinational enterprise can be overwhelming. This “relationship” is a puzzle of legal entities, ownership structures, and contractual nuances, details of which are captured at various stages of the client lifecycle. As a result, the customer due diligence process evolves over time – from onboarding to transaction monitoring – and is often confined to operational silos. These silos exacerbate fragmentation, causing critical details to be missed and creating conflicting versions of the same client record across the organization. In the absence of a central foundation for knowledge sharing, decision makers operate without crucial data that is both current and accurate.

Similar fragmentation and complexity seep into anti-financial crime functions operating across different geographies and regulatory frameworks. Faced with a cross-jurisdictional patchwork of rules, requirements, and processes, many financial institutions are forced to decentralize operations, in part because their existing systems cannot adapt to different frameworks while remaining connected to a common base. Local business units become effectively untethered to the broader enterprise from both a data perspective and an operational perspective: information, workflows, and controls do not permeate anti-financial crime operations. This enables placement and layering activities and leaves local business units and the global financial institution susceptible to financial crimes.



Copyright © 2022 Palantir Technologies Inc. (“Palantir”). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

Challenge in Focus

The potential consequences of a decentralized view were apparent in a case involving drug cartels that successfully infiltrated the Mexican unit of a multinational bank, capitalizing on the siloed anti-financial crime functions stemming from the institution's operational structure. To begin with, significant AML failures within the Mexican unit created weaknesses for nefarious actors to exploit. Furthermore, the U.S. arm of the bank failed to implement sufficient policies, procedures, and controls to detect and report suspicious activity (particularly relating to foreign correspondent accounts).

As a result of these failures, the bank missed purchases of billions of dollars of physical U.S. banknotes, as well as trillions of dollars in wire transfers from customers in countries that were categorized as "standard" or "medium" risk by the bank, including over half a trillion dollars from the Mexican unit. Perhaps the most egregious violation, however, was the failure of the group entity to inform the U.S. unit of known compliance issues at the Mexican arm, meaning the unit had minimal accountability to headquarters. In the absence of controls that propagated through the bank's systems and linked to a centralized foundation, personnel could instantiate their own policies and procedures, and alerts regarding suspicious activity did not flow through the reporting chain. Anti-financial crime violations stemming from this arrangement resulted in over a billion-dollar penalty for the financial institution.

02 Volume & Complexity →

Financial institutions widely struggle to make sense of a continuous flow of disjointed information about their customers. Ever-increasing complexity can overwhelm anti-financial crime operations, leading to costly failures.

Further complicating organizations' efforts to maintain an accurate view of their clients is a three-pronged multiplier effect that takes place throughout the course of even the simplest relationship. After onboarding, new customer data points are continually generated as:

- The customer transacts
- The customer's financial network evolves
- The customer's profile attributes change over time

This amounts to a deluge of data assets being generated by internal and external systems at any given moment. In the absence of a strong framework for capturing this data, integrating it into a single platform, and mapping it into a digestible format, there is a backlog of noisy, effectively meaningless information that is dumped into data lakes and warehouses — or worse, siloed in a single system or never captured at all. Combing through these troves of data is a constantly compounding challenge that can inundate anti-financial crime operations, especially those with outdated alerting methodologies. With mounting alert and case volumes, there is a heightened risk of true positives remaining unactioned.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

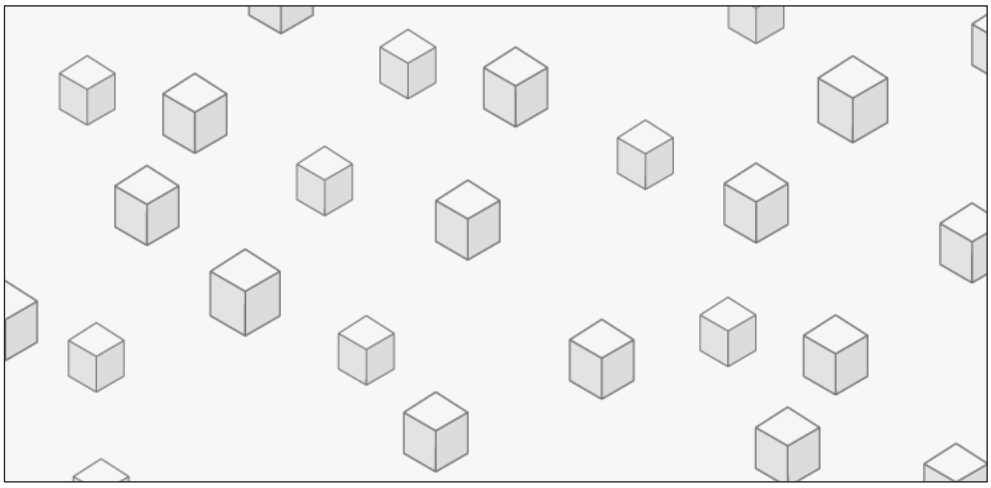
03 Legacy, Isolated Systems →

Financial institutions continue to use legacy systems for a variety of reasons, from regulatory requirements to complex interdependencies built up over years of continuous use. This gives rise to risks stemming from: (i) the weaknesses of the systems themselves, and (ii) the isolation of individual systems, which leaves financial institutions with a set of siloed, narrow perspectives.

Many financial institutions have amassed a complex landscape of workstreams and platforms spanning KYC, fraud, transaction monitoring, investigations, and more. Operating in discrete environments results in some degree of, if not total, isolation. This creates another multiplier effect: as one system generates or ingests new data about a given client, it is effectively invisible to the others. Financial institutions risk missing crucial signals due to an incomplete and inaccurate understanding of risk.

These organizations have often adopted their technologies piecemeal, and at various stages of their respective digital transformation journeys; many systems are so entrenched (or so challenging to alter) that migrations or revamps are all but impossible, and integrating data requires time-consuming manual efforts. This may leave financial institutions with both a fragmented data landscape and outdated methodologies. Demonstrating the severity of the problem, many are still reliant on the same risk and alerting logic that was in place 20-30 years ago, burying analysts in false positives and further compounding the risk of overlooking emerging threats.

Even as they seek to modernize, financial institutions frequently find that there are few solutions which can integrate with and augment their existing platforms. For many, a complete overhaul is not an option — there are certain systems and applications that must remain in place. In addition, transitional gaps in coverage while old systems are wound down and new systems come online are too risky and disruptive, leaving few paths forward.



Copyright © 2022 Palantir Technologies Inc. (“Palantir”). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

04 Reliance on Black Box Systems →

Many financial institutions rely on platforms and models that are effectively black boxes, weakening their position with regulators and increasing the risk of undetected biases and missed signals.

Due to deep entrenchment and vendor lock-in, financial institutions are effectively forced to use black box systems with unintelligible operations. Beyond the risk of undetected inaccuracies, these systems invite regulatory risk and added scrutiny, as financial institutions cannot produce evidence for their decision-making. This problem is especially acute in the models that many organizations use for their alerting systems. Unable to interrogate model algorithms or maintain a defensible position on model risk governance, they are blind to potential biases and cannot explain what factors contributed to an alert being triggered (or not triggered, as the case may be).

Financial institutions' inability to fully comprehend, document, and in some cases tune their systems can cripple their efforts to detect nefarious activity and increase the risk of exploitation. To date, financial institutions have been generous in their trust in such systems to accurately audit and document regulatory-relevant actions, as they have been more tailored for operational objectives than compliance obligations.

05 Insular Focus →

Without centralized, dynamic connections to external data sources and a built-in means of integrating this information into a unified client picture, even financial institutions that have harmonized their own anti-financial crime systems operate with an incomplete view of risk.

Many financial institutions have external feeds to inform discrete processes (e.g., negative news screenings), but few are equipped to seamlessly integrate a fluid array of outside sources and marry this data with information from their own systems. Without this capability, financial institutions are vulnerable to emerging risks, as they not only lack the infrastructure to integrate external data consistently and programmatically, but also to operationalize these insights.

This insular perspective can extend to a geographical level; financial institutions operating in multiple jurisdictions often struggle with dynamic customer enrichment. Bad actors seeking to exploit regulatory loopholes and weaknesses by coordinating their efforts across borders already have an advantage, as organized criminal groups and illicit actors are not subject to stringent regulatory requirements. Financial institutions that cannot make connections between customer activity in different jurisdictions and meet ever-evolving regulatory demands are set up for failure in an increasingly interconnected world.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

06 Assembly Line Approach →

One-directional flow of information inhibits collaboration, limits learning, and leaves systems static.

Financial institutions' data ecosystems are frequently constructed such that information moves from one function to another in sequence, limiting opportunities to improve or enhance controls and processes. The feedback loop is effectively closed off; from correcting inaccuracies to informing future decisions, critical information does not flow back into systems. This can result in both missed opportunities and damaging operational shortcomings. If, for example, an alerting system continued to generate flags even after analysts had determined that type of alert was a false positive, their attention remains diverted to a mountain of unproductive work.

An assembly line approach within the solution architecture can also mean that signals of declining productivity and increasing complexity in investigative outcomes go unnoticed until after it is too late. Without the ability to aggregate and interrogate risk levels across dimensions (e.g., PEP, negative news, sanctions, transactions, etc.), financial institutions are effectively blind to potential breakdowns within different functions of their anti-financial crime operations.

Systems that lack the infrastructure to incorporate analyst activity and actions on alerts into the broader view for any given client profile can leave financial institutions with an inaccurate picture of risk; the picture generated by analysts' handling of alerts may be very different than the client's static profile. To ensure systems are producing accurate and actionable outputs, financial institutions need solutions with feedback loops that can dynamically incorporate and operationalize new information into a multi-dimensional view.

Challenge in Focus

A large American bank was vulnerable to bad actors seeking to exploit its "assembly line" approach to AML processes. The bank in question, which has since been acquired, was issued the largest penalty ever imposed at the time for a violation of the U.S. Bank Secrecy Act (BSA). The bank's failure to maintain an effective BSA program allowed drug cartels to move over $400 billion in unmonitored funds to accounts at the bank via a network of currency exchange providers in Mexico. The bank was aware that there was a high risk of illicit funds being laundered through these currency exchange providers, yet it expanded its business with them, failing to conduct appropriate monitoring as required under the BSA. The issues began to emerge when narcotics were detected aboard a plane. Investigators identified the plane's owners before linking the movement of funds between the bank and the currency exchange houses. This case was the antithesis of how financial institutions are expected to support law enforcement: instead of providing actionable intelligence to identify drug traffickers, investigators followed the money to find the facilitators.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

07 Information Security Risks →

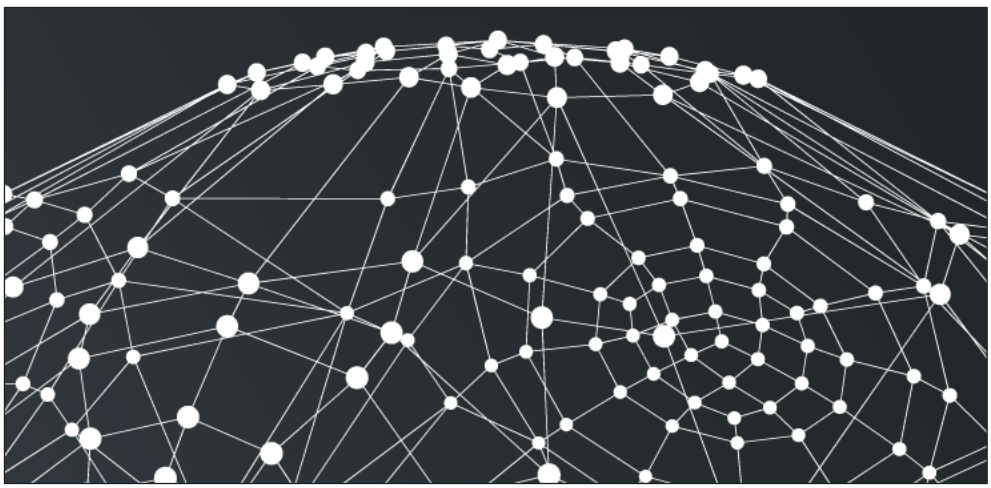
Financial institutions face evolving threats from both internal and external actors seeking to exploit any weaknesses in anti-financial crime operations, leaving them vulnerable to extensive damage.

Financial institutions hardly need to be reminded of information security risks; from infiltration by hackers to intentional misuse by employees, they are contending with increasingly sophisticated actors who can often conceal their actions even as they wreak havoc. Protecting against these risks has become an increasingly complex endeavor requiring an array of security protocols that financial institutions' systems often lack.

Take, for example, insider threats. Without robust, highly specialized access controls, employees may have access to information that they do not explicitly need, which can in turn be leveraged for nefarious means. Without a means of monitoring and generating a complete audit trail for all activity, detecting misuse of systems is extremely challenging – bad actors may inflict extensive damage before they are caught.

Anti-Financial Crime 360 with Palantir Foundry

Palantir Foundry is an open, extensible, scalable system that gives financial institutions full transparency and control over all inputs, allowing them to construct a unified compliance ecosystem and understand their risk posture at various levels of granularity – from a KYC or transaction monitoring system to an aggregated client view – and to implement specific, tailored strategies in pursuit of their anti-financial crime goals.



Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

01 Single Client View; Entity Resolution →

Foundry enables financial institutions to take a holistic, dynamic view of risk, and to constantly build an all-encompassing profile for each client. This profile both informs internal decision-making and serves as an auditable record, showing the evolution of the institution's risk assessment while providing support for each decision along the customer journey.

Underpinning this capability is Foundry's ability to continuously harmonize disparate data sources. It comes equipped with out-of-the-box pipelines for common customer, transaction, and third-party risk platforms, and can also serve as an easy connection to a centralized data warehouse or other data systems in real time or in batch. The resulting 360° view incorporates all known information about the customer, bringing relevant data from varied sources into a single, fused picture to ensure that decision makers have all risk-relevant information at their fingertips.

Impact in Action

One global bank automatically resolved four billion customer records spread across more than 15 worldwide jurisdictions — accessing customer information is now 90% faster and 95% lower cost.

02 Augmented Intelligence →

One of Foundry's strengths is its ability to help extend and enhance financial institutions' existing systems. Rather than replacing platforms and data sources and fracturing sources of truth, Foundry augments the overall anti-financial crime stack.

Foundry comes equipped with standard, documented RESTful APIs and JDBC/ODBC drivers at every layer of the platform, allowing access to the data layer by third-party tools such as proprietary transaction monitoring systems. In this context, for example, integration would include taking in all alerts generated by the transaction monitoring system along with as much data as possible (e.g., linked transactions, reasons for alerts, disposition of alerts) and tying it to existing knowledge assets on KYC, sanctions, fraud, credit risk etc., at an entity level.

Foundry can also write back to core banking, transaction monitoring, and customer systems, either in batch or individually, ensuring that these sources of truth are never fractured and benefit from the latest updates, learnings, and insights. One common use case is to write data back to core customer systems after the entity resolution engine has resolved various matches to a single customer, providing a financial institution with a better understanding of their customer base that can benefit the rest of the organization.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

03 Access Controls →

Even with state-of-the-art systems in place, financial institutions face risk from their employees – whether from negligence, inadequate training, willful misconduct, or otherwise. Robust access controls are among the best tools to mitigate insider threats, as they serve to not only limit the damage rogue actors can cause, but also to potentially prevent their actions in the first place.

To that end, Foundry comes equipped with a granular access control framework that allows financial institutions to secure information at the dataset level, down to row/column-level permissions. For each individual resource, organizations can define the users who are permitted to discover, read, modify, and delete data. In addition, Foundry's policy enforcement system dynamically manages access and usage constraints, with inherited security policies that propagate down entire pipelines: financial institutions can ensure that controls flow throughout the system, even as new sources are added and created.

In Foundry, administrators can tailor access based on employee role and responsibility. Further, it allows for easy tracking, auditing, and governing of critical data assets, not only at an operational level, but also from the point of connection itself. This allows financial institutions to control how analytics account for different permissions, meaning that they can rigorously audit and ringfence the consumption of jurisdiction and/or line of business-specific assets.

04 Scale →

As new risk data emerges, clients are onboarded, and products change, it can be challenging to stop disorder from crippling the ability of any platform to generate meaningful insights. Foundry provides numerous mechanisms to manage the immense volume, complexity, and variety of information that financial institutions contend with.

Foundry can operate across virtually any type of data – including flat files, images, and geospatial data – and can do so at scale, taking advantage of its distributed computing cluster. No matter where an organization is in its digital transformation (or where its different business units are), Foundry can harmonize data from various systems spread across product lines, business units, etc. – even if data types are vastly different — and can intelligently build, schedule, and manage petabyte-scale pipelines.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

04 Scale (continued) →

Its data integration and versioning capabilities ensure that data is modeled in a scalable way, and all data lineage is fully transparent as it moves through the system. At any point, a user can drill down on a data point and see exactly how it was derived.

Foundry allows financial institutions to unlock collaboration across technical and non-technical users, connecting teams through rich change management, discoverability, and sharing features; users of all technical abilities can also manipulate, analyze, and act on data via intuitive, interactive applications. In a modeling context, Foundry enables non-technical users to simulate, visualize, and evaluate model-based changes and “what-if” scenarios. By empowering users and facilitating connections across teams, Foundry provides a common foundation for the entire organization; analysts’ simultaneous use of the platform allows them to drive independent value over time, further enhancing its power.

In addition, Foundry’s out-of-the-box data connectors and easy-to-configure schedules, success criteria, and permission models operate alongside robust pipeline orchestration and data health monitoring capabilities, ensuring that financial institutions are able to implement infrastructure that enables their platforms to scale without compromising data integrity. This provides them the flexibility to innovate in their core business areas, adopt new products/channels, and expand to new geographies: they have a robust mechanism to measure risk that dynamically scales with their evolving needs.

Foundry goes beyond providing mechanisms for organizing and controlling data flows while ensuring data quality, however. It constructs an enterprise-wide semantic layer that effectively translates raw data into a recognizable language for end users. It does this by organizing data into objects (e.g., customers, accounts, transactions, etc.) with associated properties and relationships. This is called the Ontology. Using the Ontology, instead of dumping information into a meaningless data lake, financial institutions are adding more detail about their customers, transactions, and behaviors over time, further enriching the data foundation. Integrating and translating this information into risk factors at the object level allows for linking disparate data under a common risk umbrella and mapping it onto a unified client profile.

Copyright © 2022 Palantir Technologies Inc. (“Palantir”). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

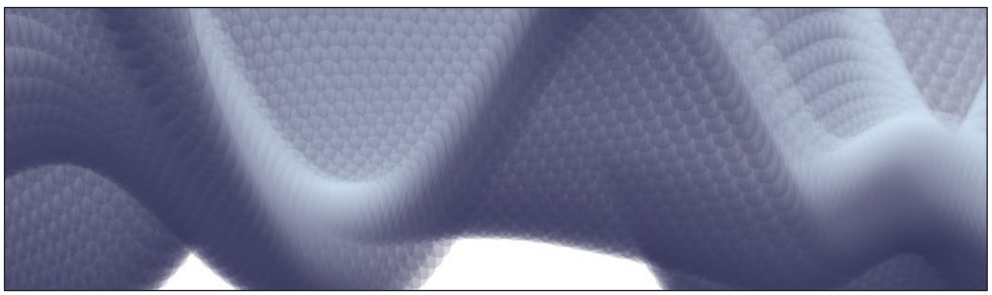
05 Real-Time Risk Evaluation →

Foundry enables financial institutions to understand risk both holistically and at various levels of granularity. It applies risk factors at multiple levels – alert, transaction, network, client, and account – allowing analysts to see a complete picture while maintaining the ability to understand the drivers of risk and quickly drill down on the riskiest entities and accounts.

Foundry is also built to be dynamic: it alerts users to significant changes in risk posture by scoring existing customers in real time as different dimensions of their profile (e.g., KYC data, transaction surveillance results) change. This allows analysts to immediately understand the changing profile of a customer and to take appropriate action, rather than waiting for retrospective reviews. Financial institutions can proactively evaluate their overall risk posture with the latest information and are therefore better-equipped to react to emerging risks.

To enable this, Foundry comes equipped with an out-of-the-box scenario manager and robust AI/ML capabilities to build, assess, and deploy models that power a risk engine. Building on the holistic customer view it has established, Foundry's risk engine incorporates all known information about any given client (including all accounts, transactions, KYC information, data from third-party sources, as well as the full network of related entities) in making a decision regarding a risk score. This risk score is typically used to calculate the priority and severity of alerts.

Beyond its built-in models, Foundry enables financial institutions to bring their own models across different risk score types (e.g., holistic risk scores, sanctions risk scores, PEP risk scores, etc.) or to create custom models. Outputs and scores from existing risk engines can be integrated into Foundry as well, giving organizations the freedom to continue using and improving their models while building others.



Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

05 Real-Time Risk Evaluation (continued) →

Just as important as core AI/ML tooling, however, is model accountability, especially in the highly-regulated and sensitive environments found in financial institutions. Foundry provides robust AI/ML safeguards through model intelligibility, verification, training data evaluation, and de-biasing. Foundry also enables financial institutions to establish analytical feedback loops, ensuring their models learn over time. To accelerate organizational learning, Foundry incorporates near-real time algorithmic outputs and captures key end-user actions and decisions as new data. The platform makes these algorithmic outputs interpretable by surfacing clear metadata, such as when the model was built, time of the most recent update, where it has been deployed, key assumptions, and performance metrics. These functions ensure that algorithms can be monitored, re-trained, and refined over time, while the underlying data foundation steadily improves across the entire enterprise.

06 Network Modeling and Hierarchy Evaluation →

As unraveling the complex web of associations stemming from any client touchpoint grows increasingly complex and high stakes, Foundry's network modeling capabilities enable financial institutions to construct a comprehensive picture of connections (whether through shared ownership, address, phone numbers, directors, registered agents, transactions, or other factors). Its investigations environment allows analysts to quickly explore these networks, understand related entities, and uncover complex transaction behavior. This environment includes graphical tools to understand transaction patterns over time, account behaviors, geolocation of entities, and other relevant information, allowing analysts to see the full picture of connected data points and relationships.

A crucial component of fully understanding customer networks is mapping the implications of ownership structures; as scandals such as the Panama Papers show, identifying ultimate beneficial owners and shell corporations in the face of increasingly sophisticated structures – and intentional obfuscation – is crucial to preventing financial crime. Out-of-the-box, Foundry's data connectors allow financial institutions to leverage third-party data sources to see a complete picture of corporate hierarchy and ownership structures, including percentage of ownership, enabling them to de-construct complex networks, understand changes over time, and identify ultimate beneficial owners at any point in a structure's history. Foundry can also help identify risk by association, tracing connections to Suspicious Activity Reports (SARs) and detecting circular flows of funds.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

07 Cross-Functional → Data Foundation

Impact in Action

Using Foundry, one payments processor integrates billions of records to understand its merchant customer base, boost revenue, and save high-value customers at risk of churn.

These insights have generated tens of millions in incremental value.

Foundry's ability to create a canonical, comprehensive client view forms a foundation that can extend across the entire financial institution, with certain core data informing operations beyond the compliance organization while simultaneously adhering to a rigorous privacy and regulatory framework. Financial institutions can leverage this 360° view for a variety of purposes, including informing:

- Next best offer analysis, preventing high-risk clients from gaining access to the most lucrative product lines, where negative impacts could be outsized
- Treatment optimization, ensuring that clients receive tailored treatment based on their revenue-generating potential and risk levels
- Credit risk analysis and collections, allowing financial institutions to see a more accurate picture of the likelihood of default and offer and/or price products accordingly

08 Operationalization → & Feedback Loops

Foundry helps to continually improve anti-financial crime operations over time by providing numerous mechanisms for the information collected, analyzed, produced, and reported within the system to be fed back into the data foundation for subsequent analysis and operationalization.

When an end user makes a decision based on an alert, scenario analysis, recommendation, or other analytical insight, Foundry captures all relevant data – including the decision itself, the business impact, possible alternatives, state-of-the-world context, and any motivating trigger, such as the alert in question. It then coordinates the capture of that information back to the financial institution's operational systems and data platform, where it informs analytics, alerting, and future decisions. This means less time spent collecting and sorting through a sea of false positives, and more time analyzing the riskiest cases.

In the transaction monitoring context, for example, Foundry makes it easy to collect feedback from analysts on which scenarios and alerts were most helpful in actioning an alert; that feedback is automatically incorporated back into the relevant model, which can improve over time as more models are tested and deployed. SARs can be analyzed so that administrators can understand exactly which factors are driving the filings and how to change scenarios or the risk model to improve the SAR generation process.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.

08 Operationalization & Feedback Loops (continued) →

Foundry has feedback loops for investigative workflows, enabling financial institutions to improve their processes over time. As with all data and workflows in Foundry, triage is clearly documented. The platform logs workflow and investigative steps to act as a feature for risk models, capturing the ebb and flow of productivity in different risk taxonomies across the customer population. Feedback can be taken from virtually any anti-financial crime workflow to improve the functioning of the system as a whole.

By providing this level of control over workflows, Foundry enables financial institutions to reap the benefits of uniting compliance and operations functions. This not only provides connective tissue that enhances decision-making, but also strong controls and clear evidence of policies being enacted. In practice, compliance teams can customize workflows and escalation paths for various alerts to specific teams or set quality control tests once a case has reached a certain level, implementing guardrails that can be propagated across the platform.

09 Auditability →

Foundry retains the complete history of all data that enters the system; versioning and provenance ensure that financial institutions can always understand and reproduce how a dataset was created. In addition, it logs all user actions, providing a comprehensive picture of both chains of decision-making and the associated context. This not only enables efficiencies in internal operations, but also provides financial institutions with off-the-shelf evidence for regulators.

10 Security →

For more than a decade, Palantir has worked with customers in the most secure and highly-regulated industries, building software for their most sensitive data. Today, security remains the cornerstone of Palantir's product development, company culture, and internal operations. Foundry was built for customers needing best-in-class security, and is capable of handling sensitive financial data, Personally Identifiable Information (PII), enabling compliance with GDPR, and more. In combination with its auditability and strong access control frameworks, these capabilities allow Foundry to facilitate collaboration while protecting against internal and external threats alike.

Copyright © 2022 Palantir Technologies Inc. ("Palantir"). All right reserved. The information in this document is proprietary and confidential and includes certain Palantir trade secrets. Unauthorized disclosure to any third party is strictly prohibited. The content provided herein is provided for informational purposes only and shall not create a warranty of any kind.