A GUIDE TO

Centralizing Data Intelligence

Discover how to modernize and accelerate the centralization of intelligence with advanced feature engineering.

DATAVISOR

Contents

Introduction

In 2020, it is safe to say we are now well past the dawning of the Big Data age. Today, every business aggregates and analyzes its data. The market is flooded with tools to help organizations try and make sense of the data they've amassed, and those with data skills are in increasingly high demand across industries.

The role of data scientist has consistently been heralded by the likes of LinkedIn, Indeed, and Glassdoor, who have routinely placed the job at or near the top of their various annual "Hot Jobs" lists for several years running. The Harvard Business Review even famously named it "The Sexiest Job of the 21st Century." Through their ability to make actionable sense of large volumes of data, data scientists have emerged as highly valuable contributors to company success. Business Analysts have seen a similar rise in reputation and value, and while they may have suffered a lack of media hype, their ranks have swelled all the same, and current estimates predict double-digit job growth for years to come. Suffice it to say that data skills remain in high demand, and businesses remain eager to glean actionable insights from the data they collect. In the field of fraud prevention, fraud and risk teams increasingly depend on advanced data capabilities to ensure comprehensive protection.

To drive continued success and growth in our modern digital economy, we must empower individuals and organizations with the advanced tools and solutions necessary to derive actionable insights at scale.

This imperative takes on increased degrees of significance in the field of fraud management, as the ability to effectively leverage huge volumes of data to power proactive detection and prevention strategies is the difference between success and failure in the face of fast-evolving modern fraud attacks.

Centralized Data vs. Centralized Intelligence:
What's the Difference?

When we talk about big data and deriving actionable insights at scale, we're talking about degrees of power, and the evolution of digital intelligence.

As our increasingly digitized world began to produce ever-greater amounts of data, we responded by developing the means to not just collect this data, but to process and analyze it. We then evolved our ability to make sense of this data, producing whole new arrays of charts, graphs, and visualizations. With each step, we grew in power. To harness this power at the enterprise level, we learned to centralize data in ways that could benefit entire organizations.

Today, in our AI and machine learning era, intelligence has become exponentially more sophisticated, and can now see a gap emerging between centralized data, and what we can think of as centralized intelligence.

With centralized data, we're still interpreting; we're still visualizing; we're still spotting trends and trying to make sense of them. With centralized intelligence, we have the power to go beyond interpretation by visualization.

Centralized intelligence is about the predictive power to create actionable insights.

With centralized intelligence, we can harness machine power to go straight to meaningful action; the machine can learn, can go through its decision process, and it can tell us what we need to do. Most importantly, the actionable intelligence resides within the system itself—it is centralized.

2 Centralizing Intelligence with DataVisor's Feature Platform

As the sheer amount of data continues to balloon, it has become increasingly challenging for businesses to manage the volume of information they have at their disposal. In response, there has been a move towards centralization—of teams, tools, and processes. At face value, this represents a positive reaction to the rising data tide. Organizations are improving their efficiency and trying to control overhead. However, the benefits are limited, as ultimately, it's still a case of centralizing data—not intelligence.

Given the demands of today's digital economy—the pressure for ever-higher rates of growth, and the competing imperatives of safety and experience—actionable intelligence derived from data has emerged as the big data era's most valuable commodity. Yet, centralization of intelligence remains an elusive goal for most organizations.

DataVisor's Feature Platform offers a solution.

FEATURE ENGINEERING: ESSENTIAL, AND CHALLENGING.

Feature engineering is critical for building any intelligent system. Features can uncover actionable insights from big data, and transform them for use by machine learning algorithms and rules-based systems. In short, features unleash the full power of big data. Without good features, creating high-performing models and rules is a virtual impossibility.

However, feature engineering is historically complex and time-consuming, with the creation of even a single, high-quality feature being a tedious, multi-step process. Given that large organizations require a large number of features to successfully address a full range of business challenges, the resources required—time, talent, systems, and more—are significant.

DATA PREPARATION → **FEATURE ENGINEERING** → **MODEL & RULES DEVELOPMENT**
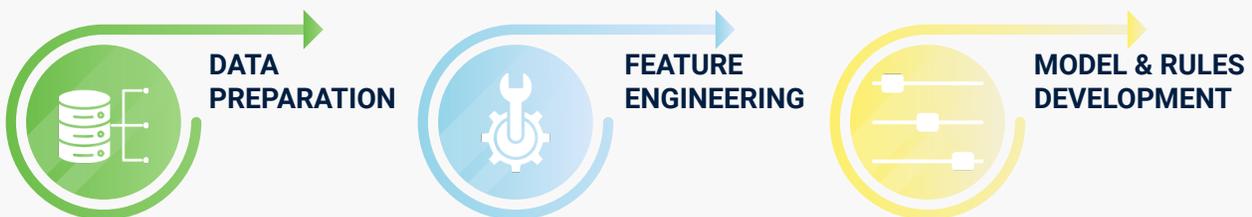
▶ Domain Expertise Required

Data scientists too often spend a significant majority of their time on the data and feature preparation phase before modeling. In a conventional scenario, data scientists analyze data and draw on their domain expertise and experience to decide what features to create. Their ongoing goal is to improve model performance, but since many features are available for modeling, overfitting—an overabundance of applied parameters that narrow, and negatively impact, a model's ability to perform— is a common problem.
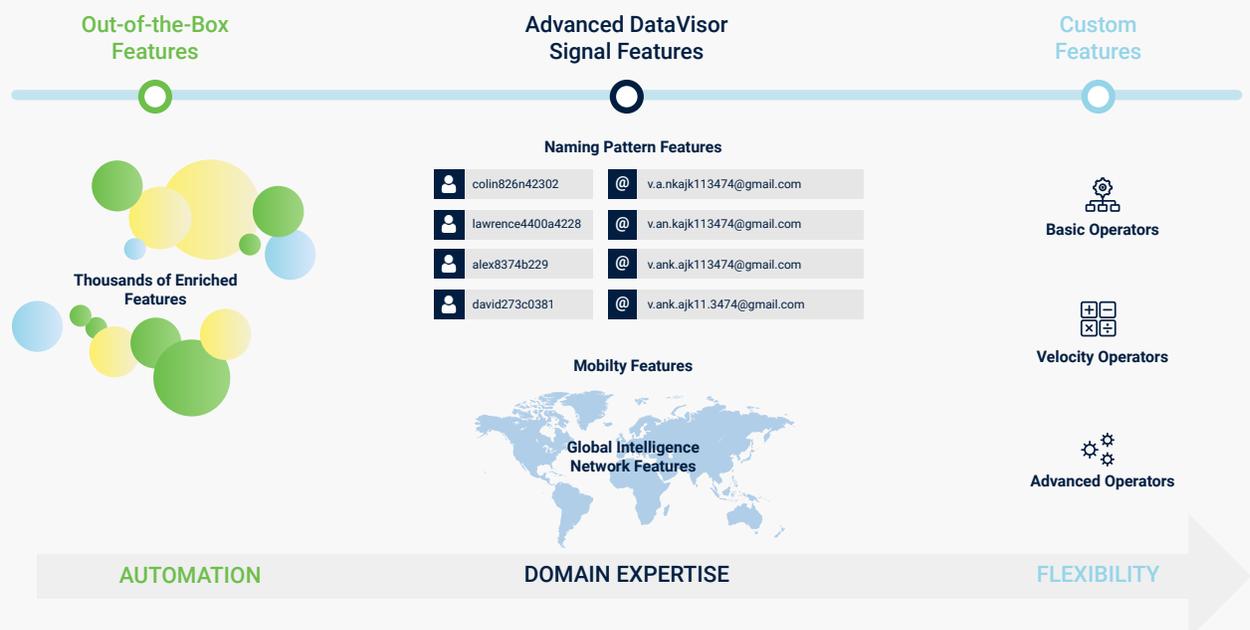
▶ Engineering Required

An additional challenge for data scientists is that when they want to build complex features and production-ready features, they usually need support from an engineering team. Creating features with complex logic—especially velocity features—requires intensive coding skills. While creating features in the testing environment may be comparatively straightforward, using them in production is another story. Data scientists often need to wait for weeks for engineers to rewrite production-ready code.

Features can uncover actionable insights from big data, and transform them for use by machine learning algorithms and rules-based systems.

▶ Computation Power Required

Creating advanced features with high velocity at big data scale requires significant computational power, as deriving actionable insights at scale is an extremely memory-hungry process. Advanced algorithms present a great deal of complexity, and real-time, holistic analysis of thousands of users and IP addresses necessitates leveraging a massive amount of computational firepower. A truly intelligent system must be optimized to perform at this level without reliance on manual processes that impede results and actions.

Out-of-the-Box Features — Advanced DataVisor Signal Features — Custom Features

Thousands of Enriched Features

Naming Pattern Features

colin826n42302	@ v.a.nkajk113474@gmail.com
lawrence4400a4228	@ v.an.kajk113474@gmail.com
alex8374b229	@ v.ank113474@gmail.com
david273c0381	@ v.ank11.3474@gmail.com

Mobilty Features

Global Intelligence Network Features

Basic Operators

Velocity Operators

Advanced Operators

AUTOMATION — DOMAIN EXPERTISE — FLEXIBILITY

THE NEED FOR FLEXIBILITY

Manual feature engineering, as described above, is labor-intensive, time-consuming, and inefficient. However, where there is a definite problem to solve and domain expertise that can be applied, it is possible to standardize certain features that can be used for building models. These features can be automatically derived or extracted from raw data. For example, IP address is essential for fraud detection. For each IP address in the raw data, it is possible to derive additional features such as: ip prefix, ip city, check_ip_from_datacenter, ip_country, and more. In this way, it is possible to develop automated processes that increase both efficiency and accuracy.

For organizations seeking to enhance model performance while optimizing for efficiency, flexibility is critical, as are empowerment and independence. Data scientists, for example, must be able to create high-quality velocity features and production-ready features without having to rely on engineering and IT support. The right balance between automation and customization is critical as well—the right solution provides optimized out-of-the-box features that can start delivering accurate results right away, while simultaneously enabling customization to further optimize performance.

ADVANCED OPERATORS

- Pre-Processing
  ✓ remove invalid values from dataset

- Event-Level
  ✓ bucketize the credit limit amount

- User-Level
  ✓ calculate the time difference between two events

- Cluster-Level
  ✓ measure the diversity of the approved credit limits within the cluster

VELOCITY OPERATORS

- The total amount of trasactions processed from a particular device within a set 7-day period.

- Difference in the price of an item compared to the avg. price of an item across platform.

BASIC OPERATORS

- Mathematical
  ✓ sum, multiply, log

- String
  ✓ convert to lower case, replace text

- Conditional
 ✓ greater than or equal to

- Logical
  ✓ AND, OR

3

A New Approach: Flexible and Efficient

A central advantage of the DataVisor Feature Platform is the flexibility it affords organizations. Not only does it deliver automated feature engineering capabilities, but it also offers the ability to custom-engineer features that are specific to organizational data and needs.

Teams can engineer any features using the comprehensive functions and operators built into the Feature Platform. Users are presented with a simple and intuitive UI that enables the creation of powerful features with just a few clicks or via simple coding, with no additional support from additional departments necessary.

Write a spike detection algorithm to check spike for a time series

- Use the aggregation function to get the number of events per IP ranges in the last 180 days.

- Apply the spike detection function to see whether we have a spike in the last 30 days.
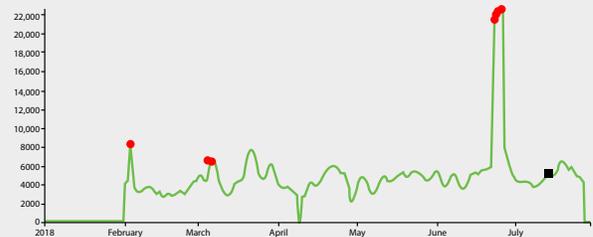
Easy Coding

- Language: Java, Python

- Support auto-complete of variable when writing

- Report complie errors

Backtesting

- Backtest the feature on data within seconds

Sophisticated Solution

- The DataVisor approach is more sophisticated than just reusing SQL UDF (user defined-function) framework.

Because these features are built in a centralized platform, the platform accordingly enables re-use and easy maintenance and allows multiple different teams to share features instead of having to start from scratch with every new business task.

Challenges

NO COLLABORATION
Different analysts create features independently and generate overlapping features.

CONFUSION ABOUT FEATURES
Users often struggle to understand how exactly the feature is created, and can only guess from the feature name.

WASTED COMPUTING POWER
Multiple derived features are computed multiple times, wasting computing power.

Feature Platform

ENHANCED COLLABORATION
Collaborators can see each other's features and understand how they are generated.

FEATURES ON TOP OF FEATURES
One person can publish the feature templates, then let others build features on top of it e.g., z score function.

OPTIMIZED COMPUTING POWER
A feature is computed only once even though there are multiple derived features from it, based on dependency.

From top to bottom, Feature Platform is optimized to enable the centralization of intelligence, and the positive results centralization can deliver.
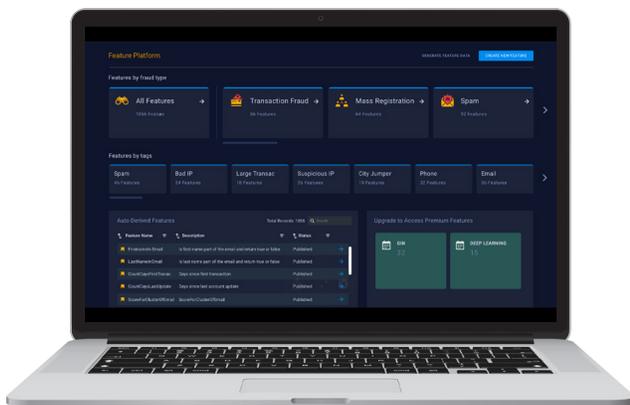
There is a difference between centralizing data and centralizing intelligence. While the former enables equal shared access, only the latter promotes and enables empowerment through the whole of an organization.

Modernization, Acceleration, Optimization

In building Feature Platform, our broad goal was to **modernize, accelerate, and optimize** the centralization of intelligence.

▶ Modern

The key to achieving this goal was making it possible for organizations to acquire, process, analyze, and act on vast amounts of data—using the power of AI and ML—in ways that promote accuracy, efficiency, and performance. We have achieved this goal by releasing a product that accelerates the all-important feature engineering process from weeks to minutes.

▶ Accelerated

With the introduction of DataVisor's Feature Platform, organizations now have access to automated feature engineering across multiple data sources, making it possible for data scientists, business analysts, and fraud and risk teams to build powerful features in minutes, instead of weeks or even months.

Feature Platform eliminates the need for intensive coding and allows teams to draw on a rich library of existing fraud features—powered by superior domain expertise—as well as to create new features themselves, adding and deploying in real time.

▶ Optimized

DataVisor's Feature Platform can recommend features optimized for a wide range of specific use cases, with an emphasis on addressing risk and fraud challenges. If an organization is wrestling with transaction fraud, for example, our Feature Platform will recommend a list of features uniquely relevant to that scenario, that can deliver strong and reliable detection results immediately.

THE FEATURE PLATFORM DIFFERENCE

For **data scientists**, DataVisor's Feature Platform offers emancipation from engineering teams, and the ability to independently build high-performance, production-ready models rapidly and efficiently, as well as to code and write scripts inside the UI for maximum flexibility.

For **business analysts**, Feature Platform delivers the power to crunch data and get insights in a matter of seconds—no queries, no coding, no third-party platforms to integrate and manage. Feature Platform provides everything necessary to derive actionable insights from raw data, all in a single UI that enables the centralization of everything from maintenance to cross-team collaboration.

For **fraud and risk teams**, Feature Platform eliminates the need for intensive coding and allows teams to draw on a rich library of existing fraud features—powered by superior domain expertise—as well as to create new features themselves, adding and deploying in real time.

	⚠ Traditional Approaches	⟳ Feature Platform
Speed	It can take weeks to create a single feature.	Features can be created in just minutes with full automation.
High Scalability and Performance	Reliance on legacy architecture prevents processing of large data volumes.	Leverages big data infrastructure to provide a scalable solution that supports high QPS.
Adding features in real time	Support for only batch processing or real-time SQL, which is slow and does not scale.	Supports adding features in real time with high performance.
Ready for production	Features cannot be directly used in production.	Enables creation of production-ready features with no IT support required.
Out-of-the-box features	No pre-built features.	Includes an extensive feature library with 1000+ built-in enriched features.
Velocity & Complex Features	IT support is required to create complex features.	Easy to create velocity and complex features with a built-in framework and via coding.
Domain expertise	Reliant on pre-existing internal domain expertise.	Leverages superior domain knowledge from global clients across 4.2B+ protected accounts.
Enhanced Collaboration & Centralized Intelligence	Different teams manage data and create features in siloes.	Enables management of vast amounts of data across teams to capture collective intelligence and monitor feature dependency.

FEATURE PLATFORM: PRODUCT BENEFITS

Feature Platform enables accelerated performance, efficient automation, and advanced detection capabilities through a unique integration of auto-derivation capabilities, deep learning functionality, and a vast amount of exclusive global intelligence data. The result is a highly flexible, all-in-one solution.

▶ **Automated Feature Engineering**

DataVisor's Feature Platform automates the feature engineering process by producing thousands of auto-derived features based on user-imported raw data and mapped fields. These features are created using attributes—such as device IDs, user agents, email addresses, and more—to provide more powerful features for advanced fraud detection.

▶ **Advanced Deep Learning**

Account-level detection leverages advanced deep learning features to surface suspicious patterns from user-generated content (such as usernames and emails) before attacks are launched, and damage is caused. Having these proactive capabilities is particularly crucial for defeating bot-scripted attacks at scale. With Feature Platform, there is no need to invest in a separate infrastructure and technology stack to benefit from deep learning technologies.

▶ **Global Intelligence**

DataVisor's Feature Platform fully integrates with our Global Intelligence Network (GIN) to further enhance feature derivation and model performance. The DataVisor GIN, powered by over 4.2B protected accounts and 800B+ events across industries, enhances machine learning engines with fine-grained fraud signals from rich digital data such as IP address subnets, prefixes, proxies and data centers, user agent strings, device types and OS, email address domains, and more.

▶ **Maximum Flexibility**

Feature Platform offers the ability to custom-engineer unique features tailored to specific organizational needs. Teams can infuse the feature creation process with their own internal expertise, ensuring even greater degrees of customization and optimization. They can engineer any features using comprehensive functions and operators, and these features can be at the event level, user level, or cluster level.
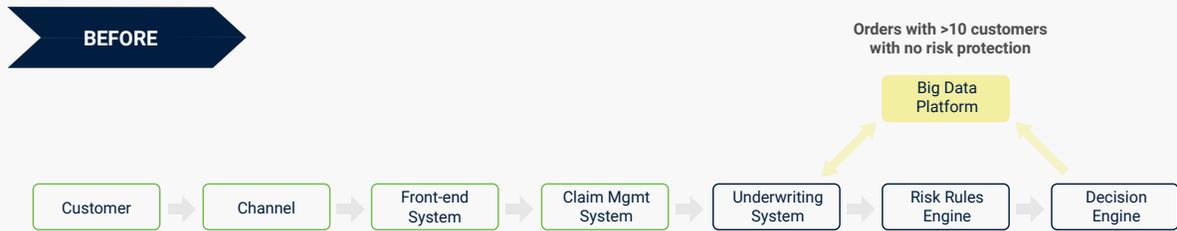
SOLVING SPECIFIC BUSINESS USE CASES

One of the core capabilities of the DataVisor approach is the ability to solve for specific use cases. The complexity of the modern digital landscape precludes the use of generic toolkits. If ever there was a one-size-fits-all solution to fraud, that time is long past. Solutions today have to tailor to every specific use case. From the first data point analyzed, through to the final step of the downstream workflow, every step must be optimized to address each unique challenge.

With Feature Platform, there is no need to invest in a separate infrastructure and technology stack to benefit from deep learning technologies.

▶ **Insurance Fraud**

DataVisor recently worked with a large insurance company to resolve the organization's inability to process big data in real time. Understanding the specific needs and challenges of the business, and how to address them, was central to the success of the effort. The process including assessing gaps between specific business requirements and existing situational realities, with examples including maximum response times being regularly exceeded, and ongoing failures to process claims where the policies had larger numbers of clients. This latter issue was an especially critical one, as, when policies had more than ten clients, risk control systems were simply skipped, with the result being the loss of millions of dollars.
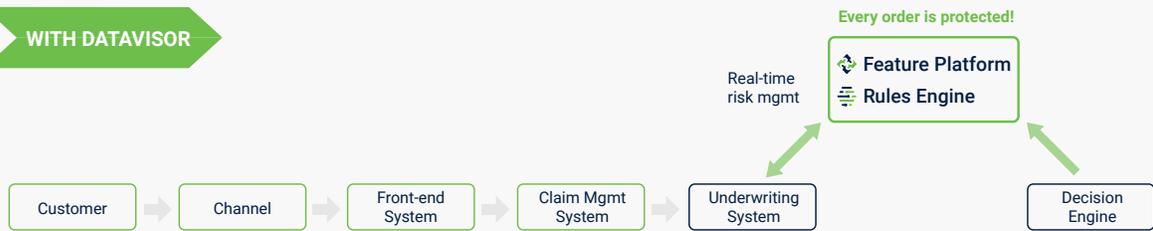
BEFORE

Orders with >10 customers
with no risk protection

Big Data
Platform

Customer → Channel → Front-end System → Claim Mgmt System → Underwriting System → Risk Rules Engine → Decision Engine

BUSINESS REQUIREMENTS:

- Max # of clients per policy: 2000
- Max response time: 500ms
- Three sets of rules to check:
  - High insurance amount
  - Apply number history
  - Duplicated plan
- Five blacklists to check

CHALLENGES: PERFORMANCE ISSUE

- Response time exceeds 1s for policy with more than 10 clients
- Policy with 10+ clients skipping the risk control systems and creating huge financial losses

WITH DATAVISOR

Every order is protected!

Real-time risk mgmt

↻ Feature Platform
≡ Rules Engine

Customer → Channel → Front-end System → Claim Mgmt System → Underwriting System   Decision Engine

DATAVISOR SOLUTIONS:

- The system is fast and can process big data in real time with very low latency; 99.9% response time is less than 32ms with 250 QPS.
- All claims can be processed rapidly and effectively, preventing potential insurance fraud.
- Integration with the client's existing solutions was rapid and seamless, and took only 6 weeks; all real-time traffic from the existing systems was successfully switched to DataVisor's AI platform.

DataVisor's audit of their systems revealed that the bottleneck had to do with volume and complexity and that the underwriting system was under enormous pressure it couldn't adequately handle.

Through a process that, in its entirety, took only six weeks, DataVisor was able to seamlessly integrate an AI-powered platform solution that enabled the processing of big data in real time with extremely low latency. Ninety-nine percent of the time, response time was less than 32ms with 250 QPS. All claims were processed rapidly, losses were significantly reduced, and potential insurance fraud

The Critical Importance of Domain Expertise

A key highlight of DataVisor's Feature Platform, as it applies to the fraud use case, is the inclusion of thousands of out-of-the-box fraud features. Making these features available puts immediate power in the hands of users, enabling teams to leverage DataVisor's unrivaled domain expertise for virtually instant results.

DataVisor has pioneered the use of AI and machine learning for fraud prevention from its inception, and today protects many of the largest and most successful organizations in the world. From leading global banks and credit card issuers, to social platforms and e-commerce sites with millions of users, to marketplaces operating in dozens of countries across the globe, DataVisor is engaged in proactively stopping new and fast-evolving fraud attacks before they launch, and before damage can happen.

Our unrivaled domain expertise informs every aspect of the solutions we offer, and our customers can confidently rely on the available out-of-the-box features to deliver excellent results right away.

Additionally, Feature Platform will recommend features tailored explicitly for use with particular fraud scenarios. Whether it's a financial institution battling application and transaction fraud, account takeover, and money laundering; a marketplace contending with fake listings, scams, and promotion abuse; or a social platform plagued by malicious bots and content abuse, Feature Platform can make available those features that are proven to deliver the best results—even against the most sophisticated and complex fraud types.
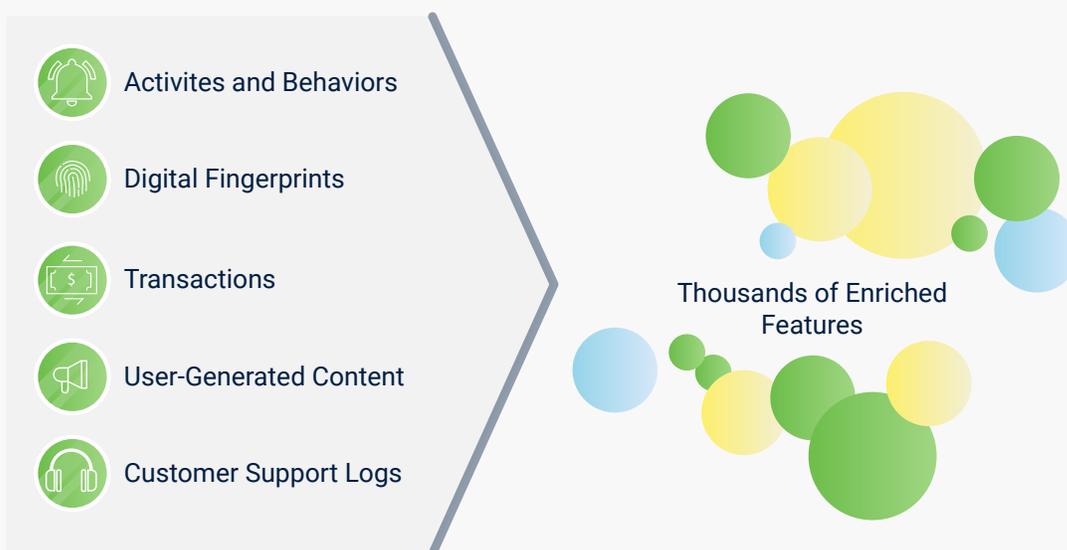
Our experience across industries and use cases is a critical differentiator when it comes to ensuring businesses can build the most optimal fraud defenses for their particular sector and scenario.

Transaction Fraud   **Application Fraud**   **Mass Registration**   **Account Takeover**   **Spam**   **Promotional Abuse**

6

Advanced Feature Engineering for Fraud

Organizations today are in dire need of advanced detection and prevention tools that can help them to protect against increasingly sophisticated fraud attacks. Data is the raw material of success when it comes to battling the complexities and massive scale of fraud that we see today. Still, without the right solutions, organizations cannot effectively leverage their data rapidly and efficiently enough to keep pace with agile modern fraudsters who can rapidly evolve their attack types. To get the model performance they need, data science and risk teams need not just big data, but the ability to uncover actionable insights from large volumes of data as well.

Even solutions and tools in and of themselves are not enough. Access to high-quality features informed by superior domain expertise is a virtual prerequisite for comprehensive coverage, as is a faster and more efficient approach.

- Activites and Behaviors
- Digital Fingerprints
- Transactions
- User-Generated Content
- Customer Support Logs

Thousands of Enriched Features

Real-World Applicability

Broad real-world applicability is one of the defining characteristics of DataVisor's Feature Platform, and as a fraud solution, it can be applied across virtually all industries. The phenomenon of call center fraud is an excellent example of this broad applicability, in that call centers are a feature of so many different businesses.

CALL CENTER SCAMS

Call center scams are a growing, industry-wide problem that cost financial institutions hundreds of millions of dollars each year:

- Contact center loss is expected to increase from $393M in 2015 to $775M in 2020.

- 61% of fraud in the U.S. can be traced back to call centers.

- Call center fraud increased from 1 in every 2000 calls in 2016 to 1 in every 937 calls in 2017- a 113% fraud rate increase.

▶ KBA

Call center security measures typically include knowledge-based authentication (KBA) questions, which are used to verify the identities of callers. Call center agents often ask callers for personally identifiable information (PII) such as home address, last four digits of a social security number, or birth date. However, the growing number of massive data breaches and social engineering attacks has made massive amounts of PII available to fraudsters. It is accordingly easy for fraudsters to obtain the information they need to beat KBA questions and successfully impersonate real customers.

▶ Mobile

The rise in mobile phone usage has presented some new options for addressing call center fraud. Mobile phone technologies allow organizations to implement security measures that rely on a variety of attributes such as IP address, browser version, and operating system. These attributes can be used to "fingerprint" mobile devices. Once on file, this digital fingerprint can be used to verify customers when they call the customer service center or use a mobile financial app. Many bank call centers rely on a combination of device fingerprinting, geolocation, and phone number information to identify a customer at the beginning of a call.

▶ A Multi-Layered Approach Is Still Not Enough

While a move towards multi-layered approaches such as these offers some improvements, they are not enough to thwart fraudsters who continue to find innovative ways to bypass these types of identity checks. For financial services providers, this is especially problematic, as financial organizations are especially vulnerable to fraud, given the increased opportunities for fraudsters to monetize their attacks.

▶ An Intelligent, Data-Powered Approach

Most financial institutions have massive volumes of data—both historical and real-time—that can be analyzed and leveraged to prevent new and emerging types of fraud. When it comes to call center fraud, for example, fraudsters often follow the same patterns before reaching a customer service representative—calling a specific customer service number, choosing certain menu options, and pressing particular numbers. Fraudsters additionally often rely on recognizable scripts when trying to scam the representatives they reach.

Using unsupervised machine learning, financial institutions can analyze their unstructured data to expose these patterns early—before any scams succeed, and before any damage is caused. This shift to proactive detention can make the difference between success and failure.

Using unsupervised machine learning, financial institutions can analyze their unstructured data to expose patterns early—before any scams succeed, and before any damage is caused.
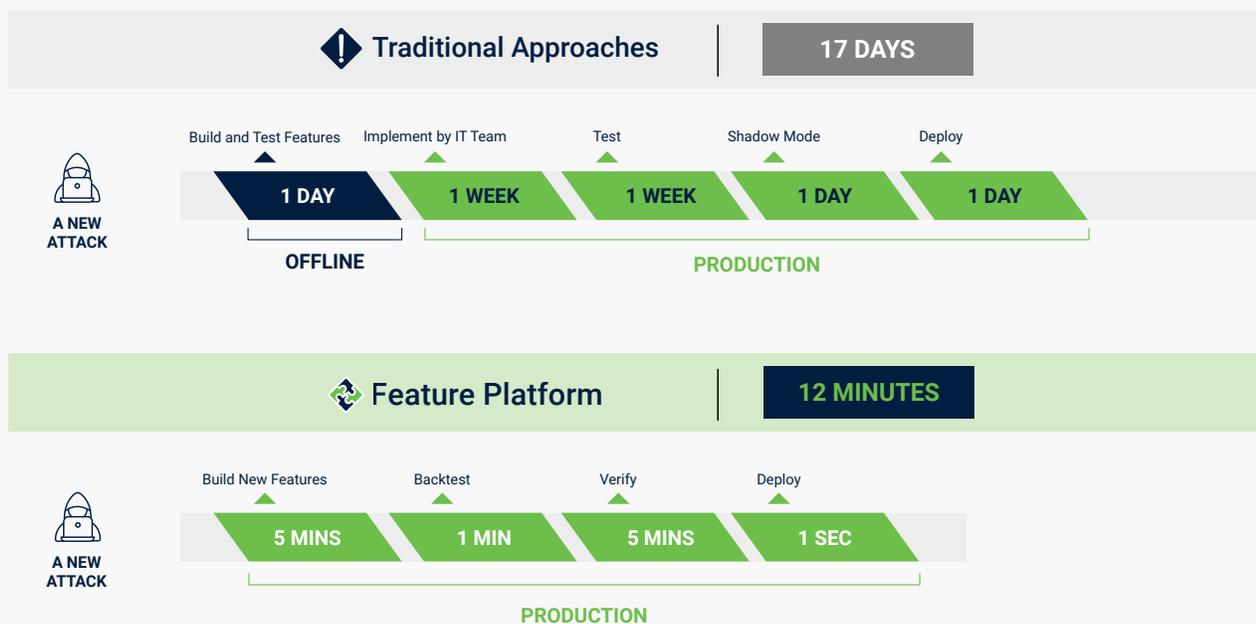
CASE STUDY RESULTS: OVERCOMING COMMON CHALLENGES

When it comes to the challenges of protecting against modern digital fraud, extensive domain expertise is invaluable. The very concept of centralized intelligence is predicated on the idea that only when the best intelligence is centrally and directly available can a system reach optimum performance. Feature Platform exists as an enactment of centralized intelligence, and its power emerges from DataVisor's years of experience deriving actionable intelligence from vast stores of enterprise client data.

This experience and expertise are why Feature Platform can reduce inefficient and time-consuming processes from months to minutes across a wide array of case studies.

▶ **New Threat Protection**

One of the most common shortcomings endured by today's enterprise organizations is the inability to respond to new threats in real-time. Traditional approaches to emerging new attack types often require two weeks or more to deploy a new and optimized model to production. The process is hampered by several factors, including extended time required to build and test new features and monitor results in shadow mode. Using Feature Platform, this process can be reduced to a matter of minutes.

Traditional Approaches | **17 DAYS**

A NEW ATTACK	Build and Test Features	Implement by IT Team	Test	Shadow Mode	Deploy
	1 DAY	1 WEEK	1 WEEK	1 DAY	1 DAY

OFFLINE — PRODUCTION

Feature Platform | **12 MINUTES**

A NEW ATTACK	Build New Features	Backtest	Verify	Deploy
	5 MINS	1 MIN	5 MINS	1 SEC

PRODUCTION

▶ **False Positive Removal**

The need to address false positives is another omnipresent concern across use cases. However, the steps required for removal are often time-consuming, as the process typically involves replacing an older, poorly performing model with a newer and better-optimized alternative. Any number of factors can cause a spike in false positives, including data input errors and problems associated with internal test data.

In these cases, a model must be changed out, and the false positives must be removed. After that, the new model must be tested before it can be deployed to production. With traditional approaches, this process can take weeks or even months. With Feature Platform, the process is reduced to minutes.

SENARIO 1:

Data Input Problem

The API couldn't collect MAC address after an update so that it used default values, triggering the model.

SENARIO 2:

Internal Test Data

A large number of internal testing requests triggered the model, creating test failure.

Generate FP

Generate FP

⚠ Traditional Approaches | **2 WEEKS TO 3 MONTHS**

Change Models → Remove False Positives → Test → Deploy to Production

Feature Platform | **20 MINUTES**

Add Pre-Filter → Add Post-Filter with Decision Engine → Config New Decision Flow

REAL TIME

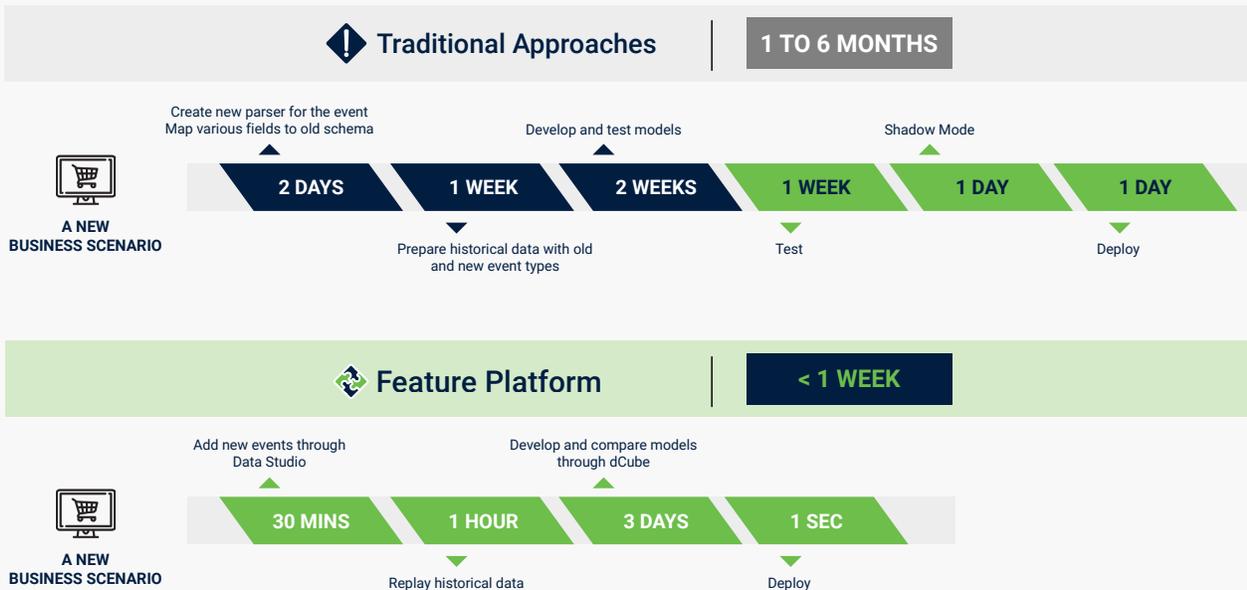Real-Time Requests → Data Correction Rules → Models → Post-Filter Rules

Decision Engine

▶ New Events For New Business Scenarios

One of the more complicated challenges is when it's necessary to add new events for new business scenarios. This is traditionally a multi-week process that involves creating a new parser, mapping new fields, and preparing historical data with old and new event types. From there, you have to develop and test new models and then test them in shadow mode.

With Feature Platform, the same results are achieved in less than a week through integrations with our Data Studio, and with dCube.

DataVisor's Feature Platform is a highly advanced tool that can be leveraged by data scientists, fraud and risk experts, and business analysts to improve results, increase speed, enhance efficiency, and reduce overhead.

Traditional Approaches — 1 TO 6 MONTHS

A NEW BUSINESS SCENARIO

Create new parser for the event
Map various fields to old schema

| 2 DAYS | 1 WEEK | 2 WEEKS | 1 WEEK | 1 DAY | 1 DAY |

Prepare historical data with old and new event types

Develop and test models

Test

Shadow Mode

Deploy

Feature Platform — < 1 WEEK

A NEW BUSINESS SCENARIO

Add new events through Data Studio

| 30 MINS | 1 HOUR | 3 DAYS | 1 SEC |

Replay historical data

Develop and compare models through dCube

Deploy

Integration

DataVisor's focus is on fraud prevention, and Feature Platform is, first and foremost, an invaluable component of any comprehensive fraud management solution. It is a highly advanced tool that can be leveraged by data scientists, fraud and risk experts, and business analysts to improve results, increase speed, enhance efficiency, and reduce overhead. This is made possible through a unique balance of automation and customization, the inclusion of a rich, domain expertise-informed library of features, and a powerful integration of deep learning capabilities and global intelligence. By enabling a centralized workflow, cross-team collaboration is seamless, with all teams working within a single, intuitive UI.

In addition to working within a complex and symbiotic ecosystem of advanced fraud prevention components, the DataVisor Feature Platform also seamlessly integrates with dCube, DataVisor's comprehensive fraud detection platform, which not only provides the necessary tools for modeling—data management, feature engineering, model review— but also automates the feature engineering process by providing hundreds of derived features based on data and mapping.

Feature Platform also works in tandem with rules engines (including DataVisor's Advanced Rules Engine), ML and decision engines, and our Global Intelligence Network, to power comprehensive coverage.

Undergirding all of this are DataVisor's exclusive unsupervised machine learning capabilities. It is these powerful algorithms that enable the flexibility required to proactively address both existing and new use cases across industries. Regardless of where challenges emerge, or what new forms they might take, it is possible to surface the patterns and correlations that indicate suspicious activity. With Feature Platform, this process is fast, efficient, and effective.
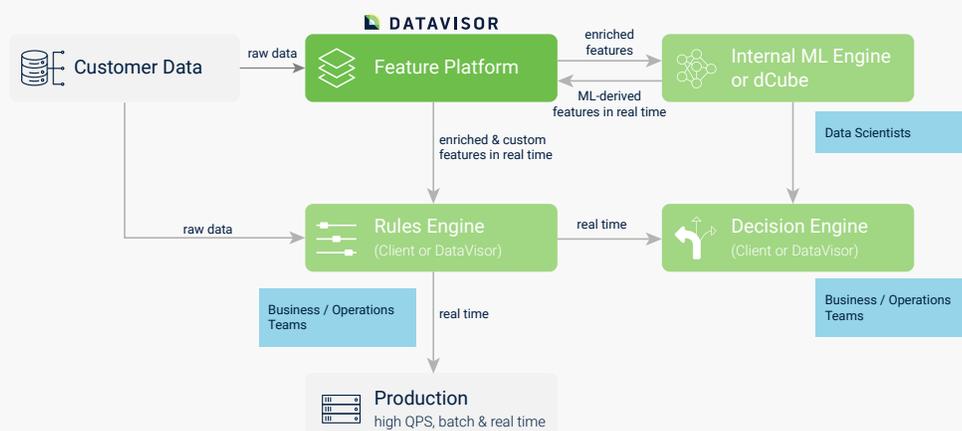
Conclusion

Centralizing intelligence is simultaneously a vertical and horizontal process. The vertical challenge is to enable every team within an organization to both contribute to—and derive actionable insights from—vast stores of data. The horizontal challenge is to make this possible across use cases and industries.

These challenges are overcome with the advanced feature engineering capabilities made possible by DataVisor's AI and machine learning-driven solutions. By empowering organizations to modernize, accelerate, and optimize the centralization of intelligence across use cases and industries, we can ensure a safer and more prosperous digital economy.

About DataVisor

DataVisor is the leading fraud detection platform powered by transformational AI technology. Using proprietary unsupervised machine learning algorithms, DataVisor restores trust in digital commerce by enabling organizations to proactively detect and act on fast-evolving fraud patterns, and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of more than 4B global user accounts, DataVisor protects against financial and reputational damage across a variety of industries, including financial services, marketplaces, ecommerce, and social platforms.

For more information on DataVisor:

✉ **info@datavisor.com**

🌐 **www.datavisor.com**

📍 967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR