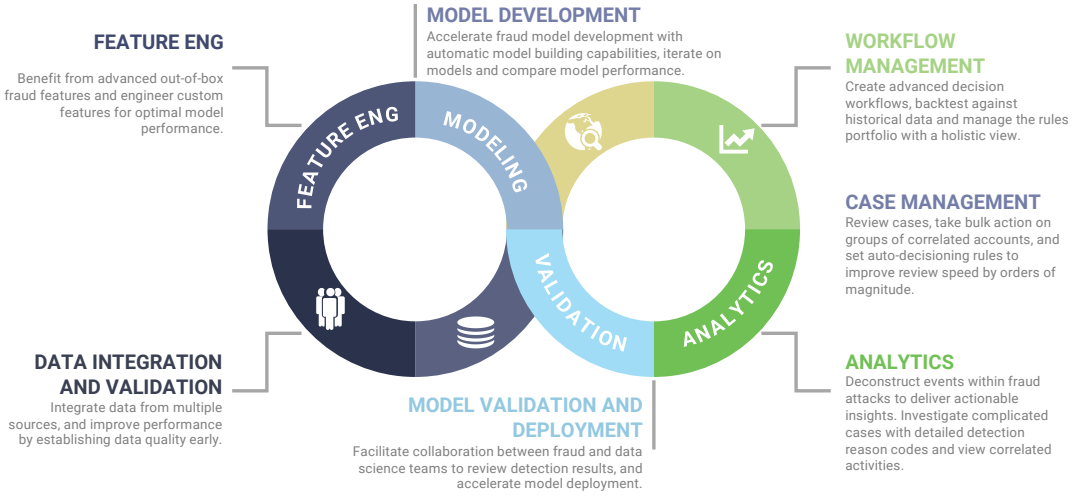
# dCube
## from DataVisor

## About dCube

**dCube is a comprehensive fraud management solution combining transformational AI-powered technology with a streamlined workflow to enable large enterprises to proactively thwart both known and unknown fraud.**

dCube features a hyper-modern architecture built to manage complex digital signals and behavior analytics using the most advanced machine learning technologies at big data scale, empowering large enterprises to identify and prevent even the most sophisticated attacks.

dCube facilitates unparalleled agility by allowing all stakeholders to collaborate on a single platform, eliminating organizational bottlenecks and enabling real-time detection and response.




## Capabilities

**Data Validation and Integration**
Accelerate fraud model development and increase accuracy by establishing data quality early. Once a user uploads their data and maps the fields, dCube automatically analyzes quality and flags potential issues; the system also seamlessly integrates data from multiple sources.

**Feature Engineering and Model Development**
Benefit from an extensive library of the most sophisticated and advanced out-of-box fraud features and automatic model-building capabilities, and additionally engineer custom features for optimal model performance in a fully automated manner.

**Model Validation and Deployment**
Facilitate collaboration between fraud and data science teams to review detection results, compare models, improve performance, and deploy in production for significantly enhanced operational efficiency.

**Decision Engine**
Create advanced decision models and workflows. Consolidate and assemble third-party signals and detection results from machine learning models and rules engines to make customized intelligent decisions and actions.

**Case Management**
Efficiently review cases, take bulk action on groups of correlated accounts, and set auto-decisioning rules to improve review speed by orders of magnitude. Access a full audit trail to view historical activity on the account, including who performed the actions, and for what reasons.

**Advanced Analytics**
Deconstruct the events within fraud attacks to deliver actionable insights alongside precision and recall analysis. Investigate complicated cases with detailed detection reason codes and view correlated activities across all accounts.

**4.1B+** Protected Accounts Globally

**800B+** Processed Events to Date

**20%** Average lift in detection

THE DCUBE DIFFERENCE

DATAVISOR

# A Powerful Detection Engine

dCube empowers organizations to accelerate machine learning adoption without the requirement of historic labels, or subsequent lengthy training and retuning periods.

With DataVisor's patented and proprietary Unsupervised Machine Learning (UML) algorithms at its core, dCube's powerful detection engine transcends simple anomaly detection (and its associated high false positives) by combining clustering techniques and graph analysis algorithms to discover correlated fraudulent or suspicious patterns that only the most advanced systems can reveal, making it possible to stop fraud in real time for even the largest enterprises in the world.

In offering a comprehensive solution built on top of a modern big data architecture that combines supervised and unsupervised machine learning with aggregated intelligence from DataVisor's Global Intelligence Network, dCube delivers high accuracy and low false positives to ensure organizations stay ahead of the most sophisticated and coordinated attacks.

**Production-Ready Big Data Infrastructure**
The detection engine is built on the latest big data infrastructure and is extremely scalable. It enables users to manage big data volume with high QPS and low latency to power real-time responses to emerging threats across hundreds of millions of accounts.

**Early, Accurate, Real-Time Fraud Detection**
Data is analyzed holistically to identify correlated groups of malicious users sharing similar attributes, enabling rapid and accurate detection of known and unknown attacks, and driving lower false positives, improved operational efficiency, and frictionless customer experiences.

**Enhanced Modeling Capabilities**
The system offers a fully packaged set of features specifically designed and optimized for fraud and risk analytics purposes, that makes it possible to create a model for any kind of a fraud scenario. Users benefit from additional flexibility to customize input data and engineer complex features that are difficult to support in a high-QPS, real-time environment.

**Workflow Efficiency**
Business analysts, fraud and risk teams, and data scientists can collaborate on a single platform, allowing for automated model development, tuning, result validation, production monitoring, and feedback loops to efficiently respond to emerging fraud attacks with the benefit of increased transparency and control.

## Deployment

DataVisor provides flexible deployment options across public cloud, private cloud, and on-premise to meet the security requirements of any enterprise.

## KEY BUSINESS BENEFITS

**Rapid Time to Value**
Bypass the need for large training datasets or loss labels and start receiving actionable detection results immediately.

**Quantifiable ROI**
Achieve high detection accuracy and low false positives to minimize costly review time.

**Seamless Integration**
Accelerate machine learning adoption through easy, fast, integration with production-ready deployment.

**ABOUT DATAVISOR**

DataVisor is the leading fraud detection company 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.