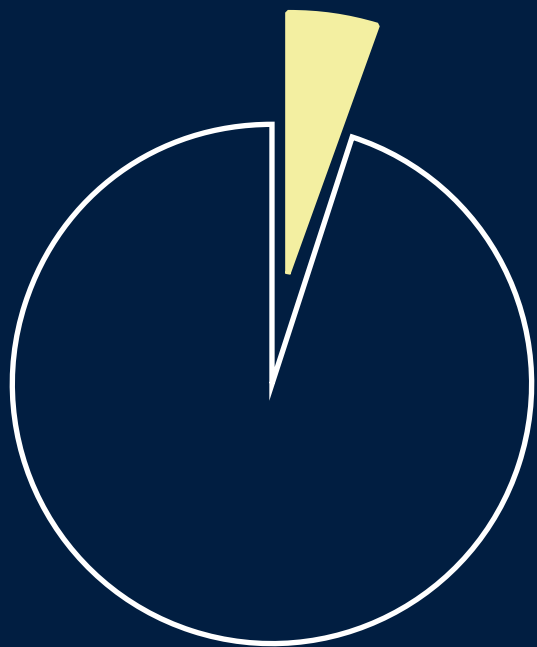


Essential Guide to Using Machine Learning for Fraud Management

What E-commerce companies should look for when selecting and adopting machine learning based solutions for fraud management





Businesses will lose an average of 5% of their gross revenues to fraud.

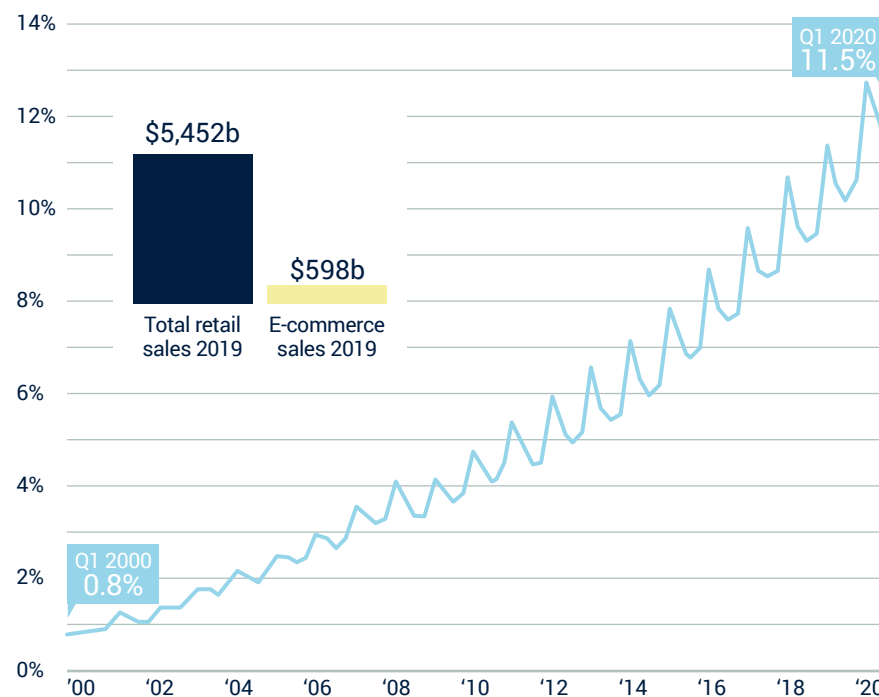
— The Association of Certified Fraud Examiners, BusinessFraudPrevention.org

Fraud costs everyone, but businesses are arguably the ones that suffer most, shelling out an estimated \$652 billion per year. That is most assuredly the case for e-commerce. As e-commerce grows, fraud losses also continue to grow.

The reason for the continued increase of fraud is that organizations are not effectively prepared to deal with the growing sophistication of fraud attacks and lack the effective tools to be able to identify, address, and stop these attacks in real time.

The Rise of E-Commerce in the United States

E-Commerce sales as a percentage of total retail sales in the United States*



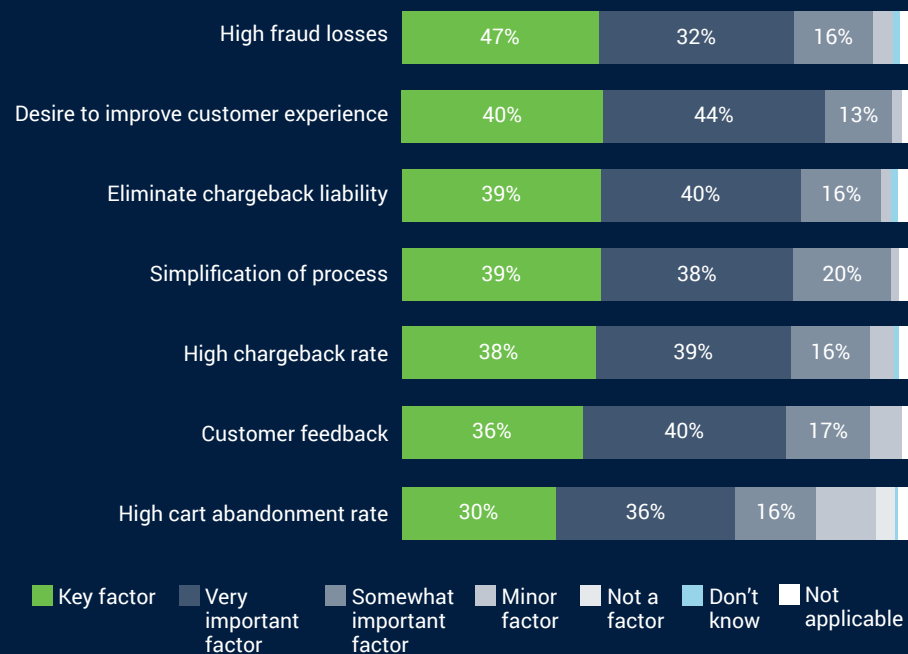
*not seasonally adjusted; excluding food services sales
Source: U.S. Census Bureau

Fraud is no longer a petty theft where an individual tries to commit a small scale fraud for minor financial benefit. With tools and technology in place, fraudsters today are highly sophisticated and, in fact, use the same machine learning that we do to orchestrate large scale attacks.

E-Commerce Fraud Statistics

- ▶ Card Not Present (CNP) Fraud is now 81% more likely than point-of-sale fraud. (Source: Javelin)
- ▶ By 2023, it is estimated that retailers will lose about \$130 billion in revenue on fraudulent CNP transactions. (Source: Juniper Research)
- ▶ From November 1-20, 2019, there were 60,000 potential online retail scams, targeting 26 popular brands. (Source: Consumer Reports)
- ▶ The cost of fraud for U.S. merchants (both store-based and e-commerce) is up 7.3% in 2020 from 2019. (Source: DigitalCommerce360)
- ▶ E-commerce retailers deal with an average of 206,000 web attacks each month. (Source: Pymnts.com)

Organizations continue to struggle to balance fraud, customer experience, and operational complexity



High fraud losses (47%) are the key factor that influences most merchants to select the automated fraud prevention solutions in use today, followed by the desire to improve customer experience and simplification of process.

No e-commerce business is safe from fraud. But even with conventional fraud detection tools in place, many e-commerce merchants struggle to keep up with evolving attacks because their tools must be retrained to protect against new threats. What's more, the money taken by a fraudster is just the beginning.

Other costs mount quickly, including the cost of lost goods or services, productivity in tracking fraud cases, reputational damage, and the need for sophisticated fraud prevention tools. In some cases, e-commerce

merchants may be forced to raise their prices for honest customers to offset the financial damage created by fraudsters.

Some of these costs are simply incalculable. One thing is clear: fraud is never a victimless crime.

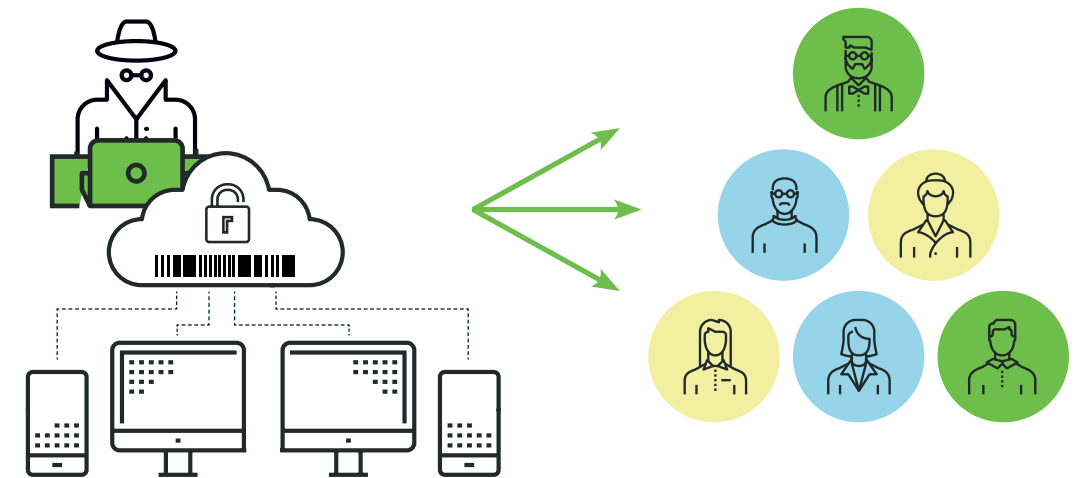
Security and risk leaders must look beyond payment fraud to establish trust and safety in all customer interactions.

Individual Attacks



Physical and individual bad guys are less popular

Coordinated Attacks With Fake or Stolen Identity



Bureau data leak -> identity theft and fake account applications
Account takeover -> fraudulent transactions

IN THIS GUIDE, YOU'LL RECEIVE:

- + Criteria to evaluate your fraud preventions strategy
- + Hidden costs of fraud detection and how to calculate fraud ROI
- + Specific capabilities that protect against new and emerging fraud attacks
- + Resources needed to deploy your solution
- + An overview of strategic business initiatives and how your solution supports them

Consider the following factors when evaluating solutions for fraud detection and prevention:



Protect Against Unknown Threats

Does the solution rely on previous-known fraud patterns and data training, or can it also detect new and emerging fraud patterns? What data does the solution need to detect fraud with high accuracy?



Total Cost of Ownership

How soon will the solution begin to add value to your organization? Are there hidden costs to owning the solution?



Required Resources

What resources are required to ensure a successful deployment for users and the organization at large? Does the solution require new and highly skilled resources, like data scientists? Can it increase the effectiveness of existing resources?



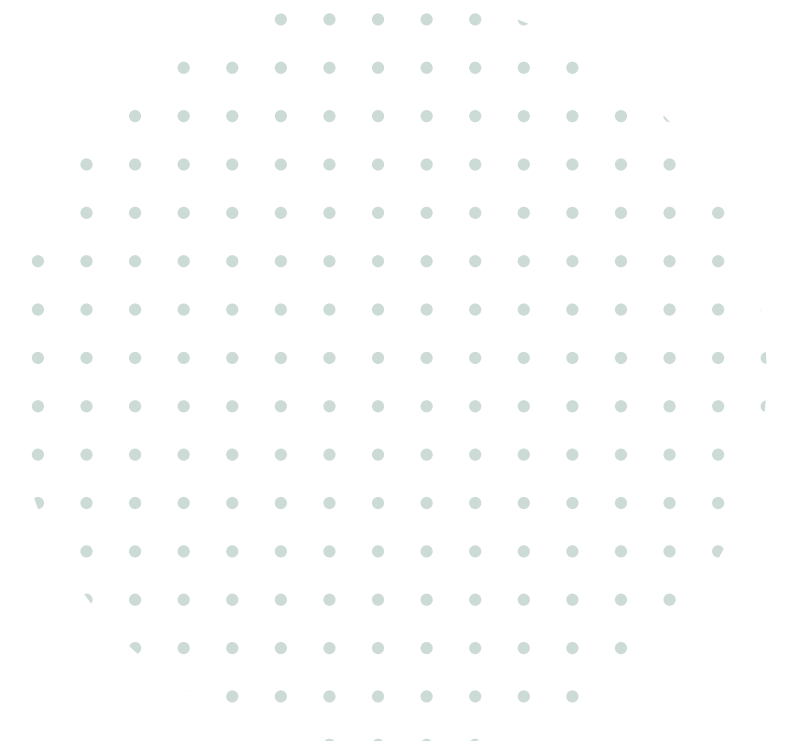
Extensible Across Use Cases

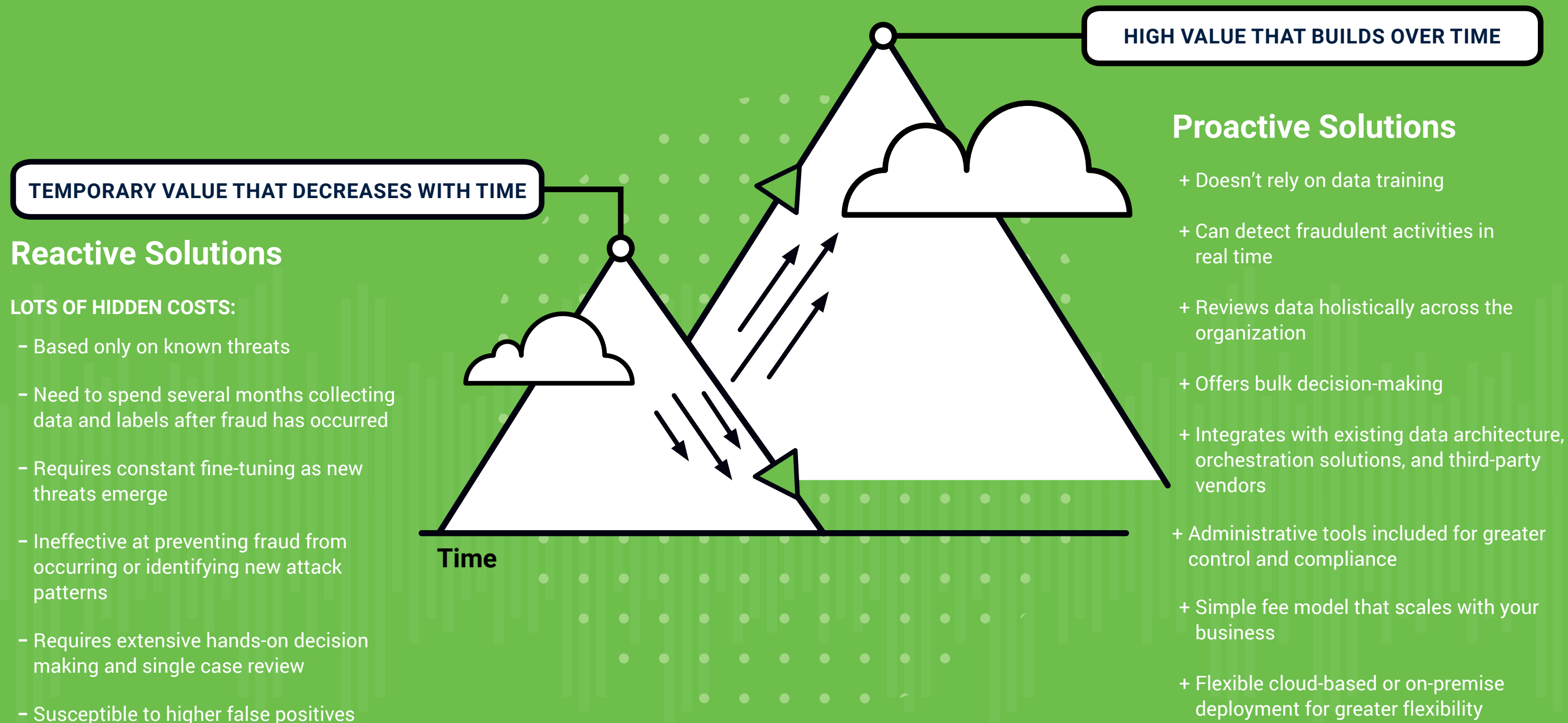
Does the fraud detection tool apply to all channels and potential instances of fraud? Does it also support your key growth initiatives?

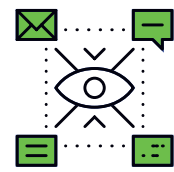


Time to Implement

How quickly can you successfully deploy the new solution? What are the costs and timeline of implementation and training your employees on how to use it?







Protect Against Unknown Threats

Powerful fraud prevention isn't limited to existing data and known threats. New methods of committing fraud are evolving as quickly as fraud detection and prevention solutions are being deployed. Prioritize tools that can help you evolve and scale your fraud detection without extensive training.

Stop Threats Before They Occur

Large-Scale Coordinated Attacks

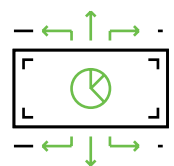
Effective fraud tools can look for large-scale coordinated attacks in real time that typically evade traditional fraud prevention measures. In many cases, reviewing single activities can evade fraud detection tools because they use seemingly authentic information. Viewing these activities on a larger scale in real time can reveal sophisticated crime rings using emulated devices and bots.

Proactive Fraud Prevention

Solutions that are proactive vs. reactive do not rely on traditional data labeling and lengthy training times. By taking a proactive approach, companies can mitigate losses related to fraud rather than try to recoup some of their losses after the fact. One report shows that companies recover less than 25% of their stolen revenue.

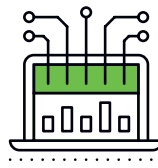
Bulk Decision Making

The window of time it takes to create an account and complete a fraudulent transaction is shortening. Fraud solutions must allow companies to take swift action to prevent fraud from occurring in the first place. This requires fast rules implementation, adding users to white lists or black lists, and taking action on groups.



To manage and maintain security, we cannot just rely on our knowledge of the known. We must redefine how we approach the problem of unknown threats.

-Yinglian Xie, CEO and Co-Founder, DataVisor



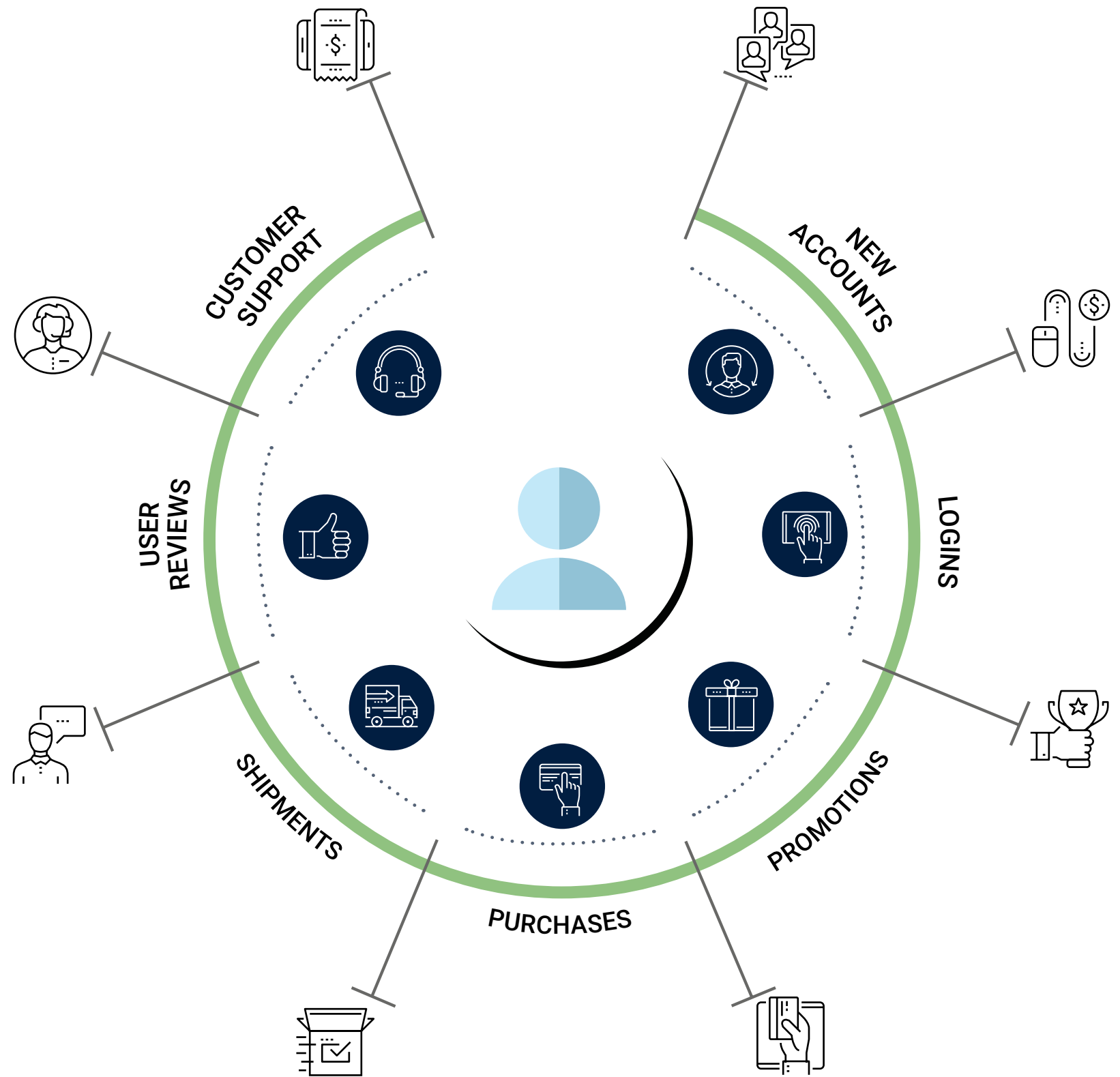
Extensible Across Use Cases

Many organizations have more than one area that is vulnerable to fraud. This is especially the case as more companies adopt an omnichannel environment. Ideally, your fraud detection solution can be applied across the enterprise to address multiple use cases.

One Tool - Any Type of Fraud Continuous Customer Lifecycle Protection

A comprehensive fraud detection solution addresses multiple potential stages of the customer account lifecycle where different types of fraud can occur including:

- ▶ Mass registration of fake accounts
- ▶ Account takeovers
- ▶ Promotion abuse
- ▶ Payment fraud
- ▶ Shipping fraud
- ▶ Content abuse





Total Cost of Ownership

The total cost of ownership, or TCO, includes all of the upfront costs and expenses of a particular solution over time. These costs include the initial purchase price, any hardware and infrastructure investments, annual licensing fees, training costs, operating expenses, customer support, and other related charges.

Upfront Costs

One of the most important upfront costs to anticipate is the fraud solution purchasing cost itself, as well as ongoing professional services. For rules-based solutions, you'll also need to consider the cost of time and resources needed for data collecting, labeling, and model training.

For a cloud-based solution, upfront costs may also include computational power, training resources, and per-user subscription access. If you are starting from scratch, your fraud teams may not have any knowledge about the type of fraud to expect. For on-premise solutions, you may need to consider server and hardware requirements, physical security, and data center personnel.

Maintenance

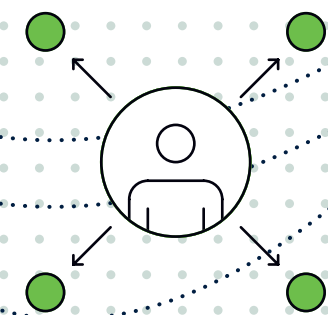
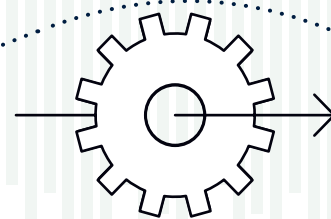
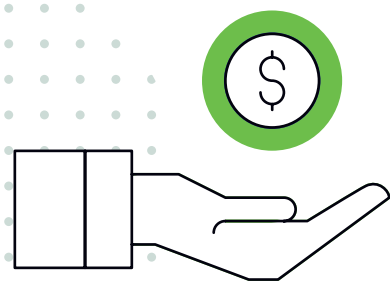
Once you build out your initial fraud model, you may need to tweak and refine it when new opportunities or weaknesses present themselves. Retuning is also required as you add or remove services or touchpoints. New patches and upgrades may also become available for an added fee.

Rules and supervised machine learning need updates every 3-6 weeks. Each time, these models go through lengthy variance and validation. Retuning is also required as you add or remove services or touchpoints.

Approaches like Unsupervised Machine Learning are self-adapting, so they eliminates many of these costs.

Vendor Support

One thing to ask about is whether support is included in your service. If so, it's a good idea to ask how support is delivered (e.g. via internet database, live chat, phone, etc.) and whether this level of support fits your needs. If support isn't included in the price, you'll need to calculate this cost into your TCO.





Time to Value

Time to value refers to the window of time between when a solution is purchased to the day the solution begins to deliver an ROI. This window can vary drastically, depending on implementation time, learning curve, and time to realize cost savings (from stopped fraud, operational efficiencies, etc.). The shorter the time to value, the faster your organization will start benefiting from the new solution and the sooner you'll start seeing an ROI.

Proof of Concept

Once you have an idea of how you want your organization's fraud detection to look and function, set up a proof of concept to put your concept to the test. This allows you to see in action how a new tool works and whether it addresses all security vulnerabilities. You can also use this time to gain valuable feedback from a select group of users prior to implementing it across your enterprise.

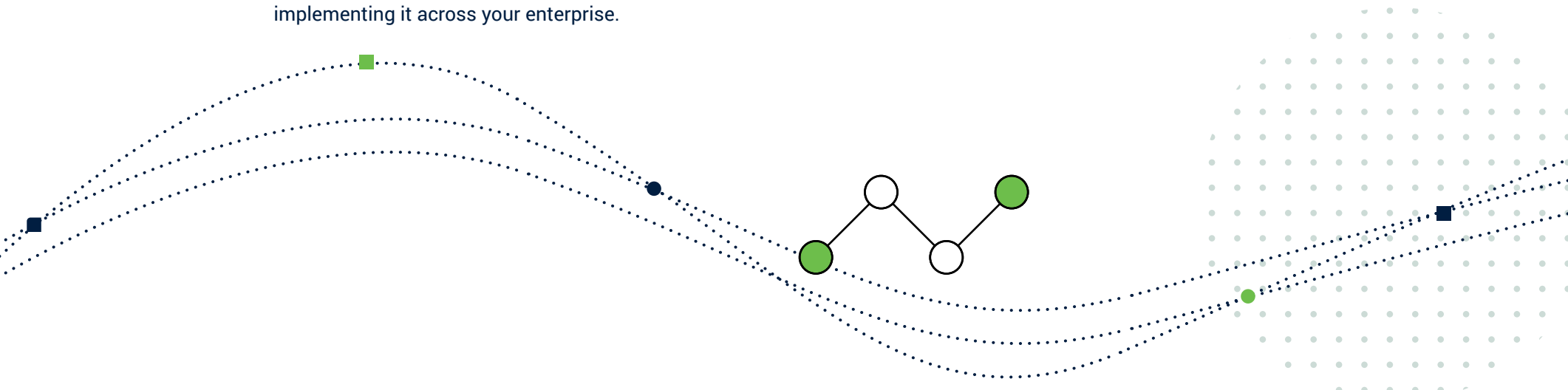
Deployment

Get a snapshot of what the actual deployment process will look like. What steps are required? How long does each step or phase take? As a general rule, cloud-based solutions will deploy faster because they do not require the complexities of hardware installation and connectivity that come with on-premise solutions.

User Onboarding & Development

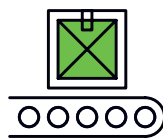
Onboarding and training the teams that will be using the software solution is critical to the process. Though the solution itself is responsible for most of the heavy lifting when it comes to fraud detection, users still need to understand how to respond to any red flags found by the system and develop best practices for how to use the data you collect.

There's also the time it takes to enroll users with the new solution. Many vendors may offer a bulk enrollment, which can save valuable IT man-hours. If this isn't an option, you may need to allocate resources for getting users set up in the system.



A fraud detection solution should include an easy-to-use API or SDK to integrate with existing systems quickly. You should be able to deploy the fraud prevention solution where needed, which could be on the cloud, on-premises, or on both.

-Hao Li, Head of Customer Success, DataVisor



Required Resources

Effective fraud detection tools work quietly in the background, but they don't function alone. Rather, to deliver the best results, your new platform will require certain types of data (the more, the better), along with skilled users, accessibility, implementation support, and other resources to continue delivering strong results. Your vendor can give you a better picture of what resources your solution requires.

Fraud Teams

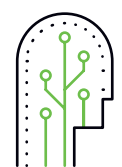
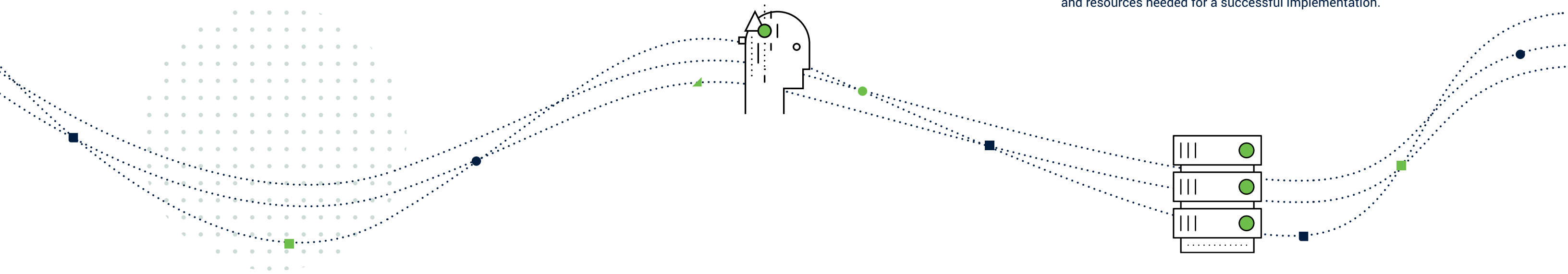
Ideally, you'll have an internal fraud team that can become the resident experts on your new solutions. These team members will be responsible for helping to train new users, monitor, and manage the platform, respond to red flags, and retune your fraud model over time.

Data Scientists

Part of your fraud team should include data scientists that can understand the data and analytics you collect and transform them into usable insights. Through the work of your data scientists, you can better understand the ROI your fraud tools are delivering as well as the vulnerabilities they solve and how they are building a stronger company from the inside out.

Data and Hardware Infrastructure

Different solutions may have varying needs for hardware and data sets to get the platform up and running. You'll need to find out specifically what type of data you need to provide as well as any hardware requirements to implement the new tools. You will also need to consider the role of your IT teams in deployment and whether they have the expertise and resources needed for a successful implementation.



Your ability to identify fraud is entirely dependent on whether you have the infrastructure in place to collect and compile relevant signals from various data sources.

-Fang Yu, CTO and Co-Founder, DataVisor



DataVisor's Comprehensive Detection Platform

DataVisor delivers a comprehensive fraud and risk management platform that protects organizations from all types of fraud.

DEVICE INTELLIGENCE:

Stop fraudsters at the gate by leveraging device fingerprints.

ADVANCED MACHINE LEARNING:

Proactively detect unknown fraud and benefit from self-adapting models

CLOUD ADOPTION:

Integrate your data easily and scale your fraud methods as your business grows.

CENTRALIZED INTELLIGENCE:

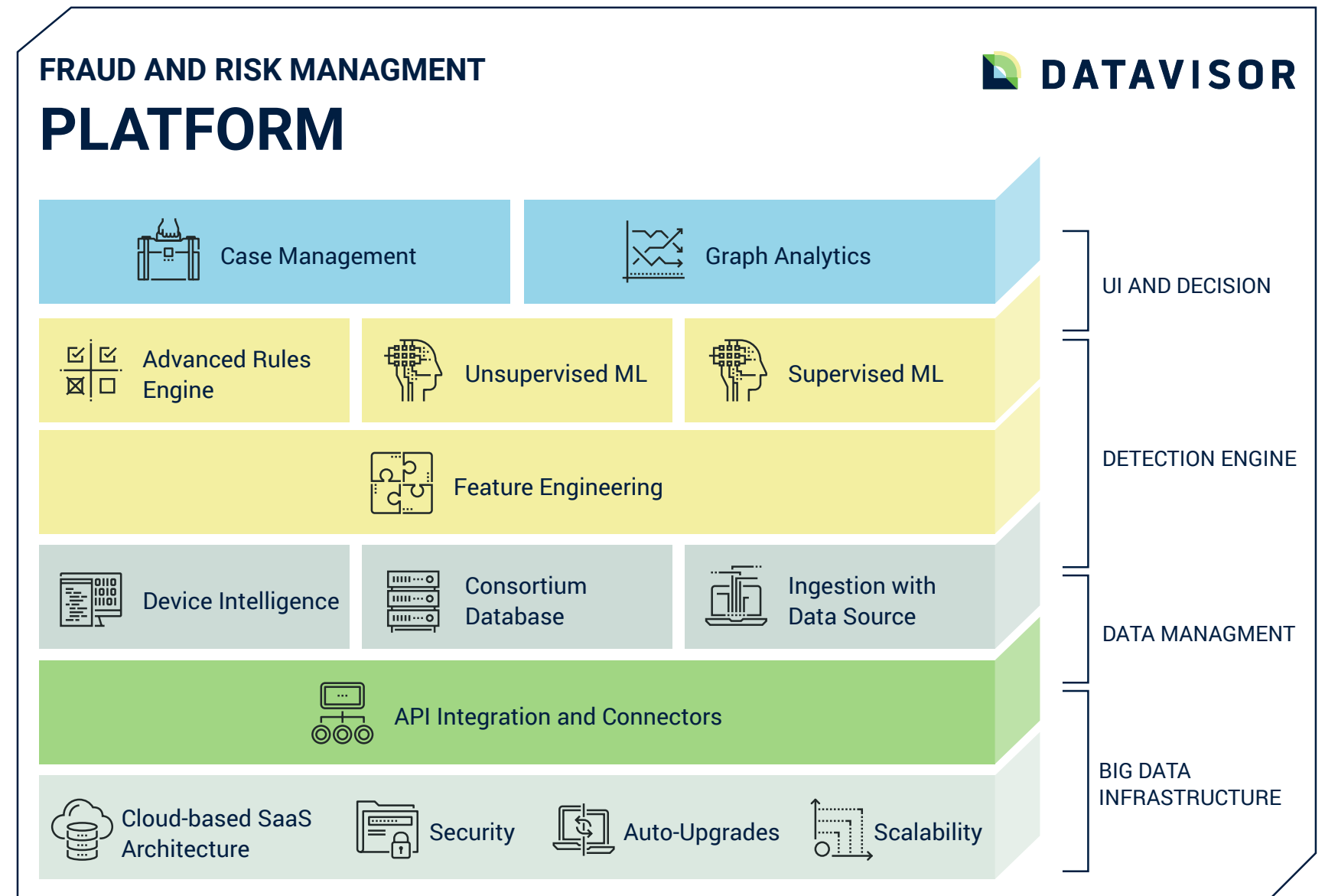
Use the same tools for multiple fraud use cases.

DIGITAL-FIRST APPROACH:

Leverage both structured and unstructured data to detect new fraud patterns and stop attacks before they happen.

REAL-TIME OPERATIONS:

Take immediate action on emerging fraud patterns without relying on IT.

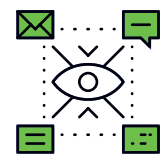




The DataVisor Advantage

DataVisor takes a unique approach to AI fraud detection through the use of unsupervised machine learning (UML). This allows the platform to not only identify and mitigate known attacks, but also detect unknown or new attack patterns that may otherwise leave companies defenseless.

Here's how DataVisor holds an advantage in each of the above criteria:



Protect Against Unknown Threats

UML

DataVisor's UML does not depend on the use of data training or known issues. Instead, it aggregates data across the enterprise in real time to detect evolving patterns and threats. This allows companies to take a proactive approach to fraud rather than waiting for fraud to occur and then learning from it for future defenses.

BULK DECISION MAKING

Because UML can identify large coordinated attacks, fraud teams can make bulk decisions instead of profiling individual cases. This helps to reduce internal costs and prevent fraud from slipping through the cracks.



Extensible Across Use Cases

USES MULTIPLE DATA SETS

DataVisor works by reviewing all data holistically in real time. By reviewing multiple data sets, the platform can better detect fraud occurring in different channels.

IMPROVES VISIBILITY

Integrating DataVisor across the enterprise gives you higher detection accuracy and delivers deeper insights into your security profile.

COMPREHENSIVE PLATFORM

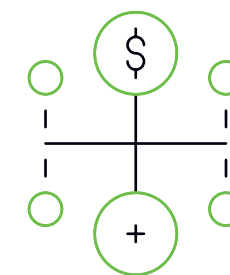
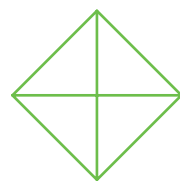
Rather than relying on point solutions, DataVisor provides a comprehensive fraud detection platform that detects any type of fraud in real time.



Total Cost of Ownership

MORE UPFRONT VALUE

Because DataVisor uses unsupervised machine learning, companies can start seeing results immediately without the need for historic labels or lengthy training times.





Time to Implement

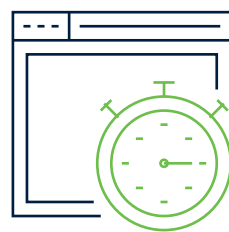
SEAMLESS INTEGRATION

DataVisor works seamlessly with your existing data architecture, orchestration solutions, and third-party vendors. Our three-step process simplifies the timeline so you can start making the most of its features:

- 1. Integrate data** by sharing a few samples to test data quality, then stream data to DataVisor's integration endpoint.
- 2. Implement DataVisor's detection system** by reviewing detection results and reason codes, then set up existing systems to parse in and take actions on the results.
- 3. Start using results** by defining the criteria of auto-actioning based on DataVisor's detection results, and attend training sessions to learn how to use the case management consoles to boost operational efficiency.

ROI WITHIN TWO WEEKS

A user-friendly interface and rapid integration significantly reduces training and onboarding time, allowing users to start seeing an ROI within two weeks.



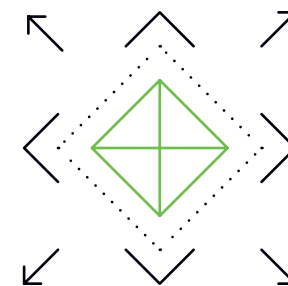
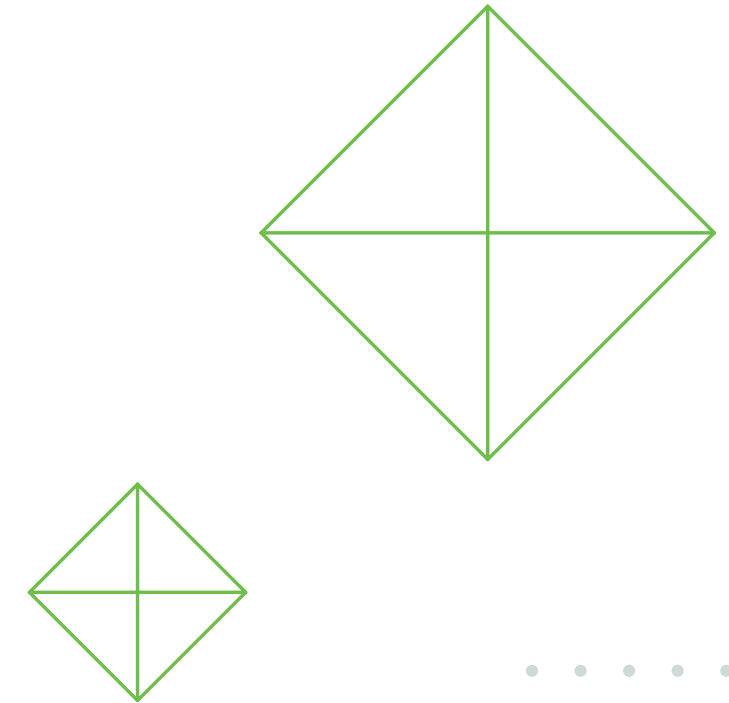
Required Resources

STREAMLINED, SCALABLE SETUP

For implementation, customers only need to provide basic data fields and user events, and our team will do the rest. DataVisor's cloud-based infrastructure also eliminates the need to upgrade or add hardware as your business grows.

ONGOING SUPPORT

Included support ensures you get the most from your DataVisor tools. Each DataVisor account receives a dedicated Technical Account Manager that can provide 24/7 support. Our team responds quickly to any issues or questions and offers as much guidance and comprehensive training as you require.



“With DataVisor and **machine learning**, we were able to **identify and stop mass scale fraud attacks** before they had any effect on our users.”

Steve Knopf, VP of Trust and Safety, Letgo

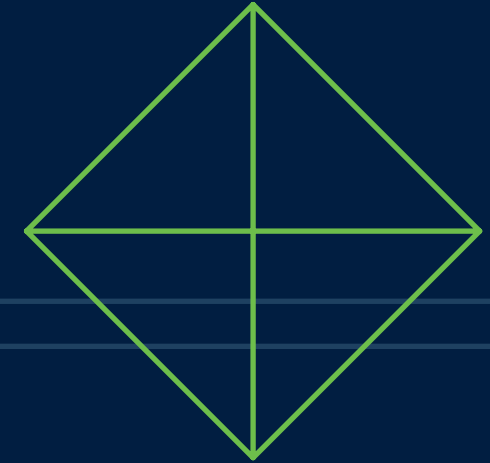
“DataVisor’s **machine learning solution** is the most critical component of our fraud defense as we grow in the digital space, **helping us minimise customer friction while defeating fraud risk.**”

Richard Cooney, Director of Fraud Strategy, Access Financial

Take the guesswork out of new and evolving threats that could be costing you a fortune and **take DataVisor’s machine learning solutions for a test drive**

REQUEST A DEMO







About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform for enterprises. 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

