Fight Fraud in a Mobile-First World with Device Intelligence

DATAVISOR

Table of Contents

Introduction

Increasing competition and a global pandemic aren't the only things threatening today's businesses. One major risk that can damage a company's bottom line (and its reputation) is the increase in fraud attempts via digital devices.

Modern fraudsters are taking a mobile approach to carry out their activities. Things like fake accounts, promotion abuse, transaction fraud, account takeovers, and content abuse (among others) are occurring on a multitude of mobile channels with the help of device emulators, app cloners, and other concealment technologies. This makes it harder for businesses to connect the dots between seemingly singular threats. This proliferation not only increases the potential loss for businesses but also makes it difficult for companies to continually adapt their fraud prevention strategies.

Because today's fraudsters are using automation and digital devices to scale their efforts, companies must also use these same technologies to fight back.

This whitepaper explores DataVisor's device intelligence solution, a mobile-first device intelligence solution that's purpose-built to face modern fraud challenges head-on.

1 The Challenges of Addressing Mobile Fraud Attacks

Mobile fraud detection has proven to be burdensome across industries. Without an effective plan to detect and prevent it, fraudsters will continue to exploit these channels at other business's expenses.

The reasons mobile fraud detection efforts have been limited are multifold:

Inability to Fight the Scale and Automation of Mobile Attacks

Mobile device fraud can occur at lightning speed, thanks to tools like bots and automation. These tools allow fraudsters to scale their efforts quickly and remain concealed with the help of emulators. When emulated devices fly under the radar, fraudsters can launch widespread attacks that quickly evolve and make it difficult for companies to shut them down.

Failure to Detect Compromised Devices

Compromised devices pose huge risks to businesses. Attackers use tools like emulators, botnets, and VPNs (among others) to conduct and conceal their activities. Attackers can also reset their devices or manipulate device parameters to obfuscate the device ID. This makes it difficult to trace activities back to the fraudster.

Creation of Friction for Good Customers

Clunky threat prevention SDK slows down app performance, which can negatively impact the customer experience and slow down transactions for good customers.

Unable to Secure Data and SDK

Traditional threat prevention SDK might be vulnerable, which could allow fraudsters to break the encryption and hijack data.

2 Leveraging Device Intelligence to Combat Fraud from Mobile and Web Attackers

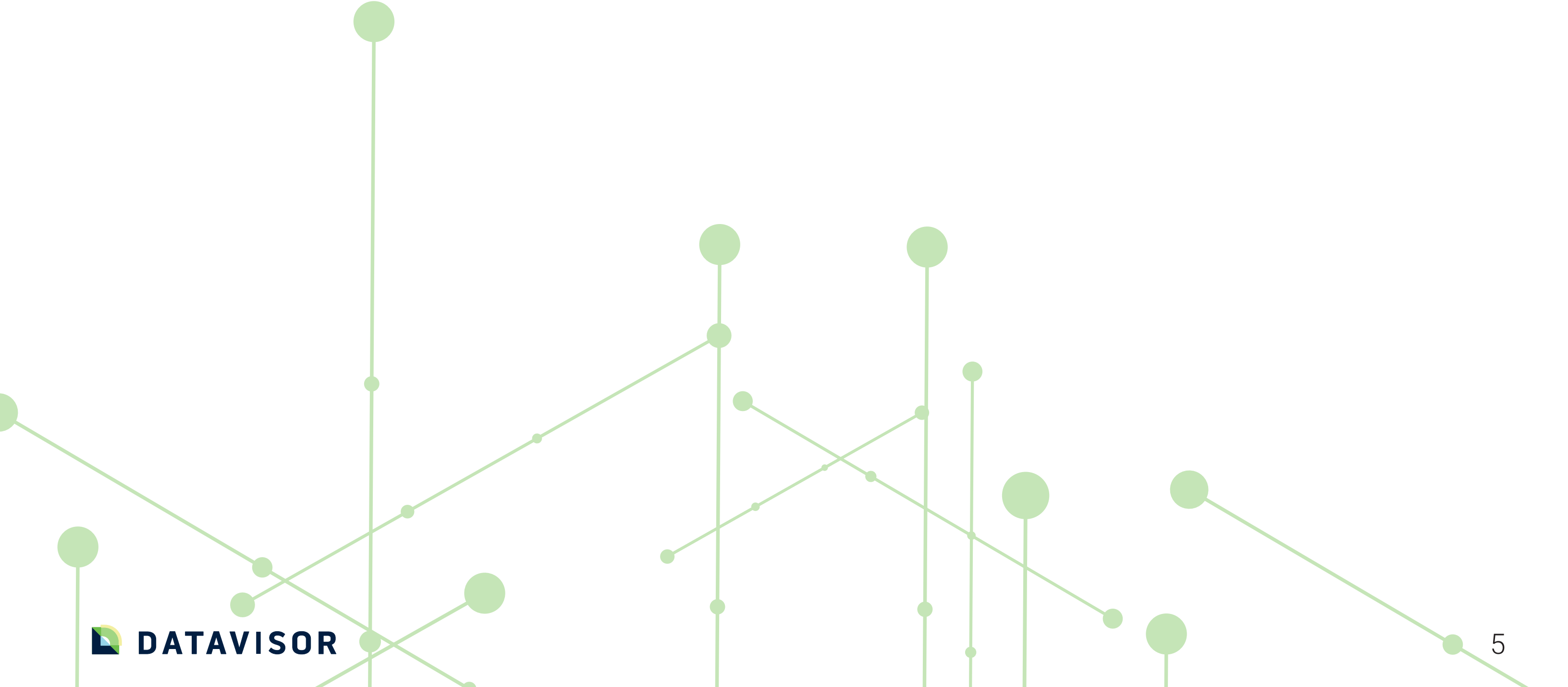
Mobile and web applications are uniquely susceptible to fraud, given the multitude of ways fraudsters can manipulate devices to carry out their activities. Advanced tactics like hook, root, and emulators can change device IDs and launch large-scale attacks while keeping things like location and identity concealed. Existing solutions are unable to effectively detect these sophisticated manipulations, and therefore allow these highly damaging attacks to slip through the cracks.

To combat the quickly evolving threats posed by mobile and web devices, businesses need real-time device intelligence that can help them identify attacks and threats immediately.

Introducing DataVisor Device Intelligence: A Mobile-First Fraud Solution

DataVisor’s device intelligence solution is a mobile and web fraud detection solution that gathers extensive device information to identify manipulated devices and risk signals, assign risk scores, and stop fraud in its tracks. The solution is built to defend against attacks from manipulated or hijacked devices regardless of the fraudsters’ techniques.

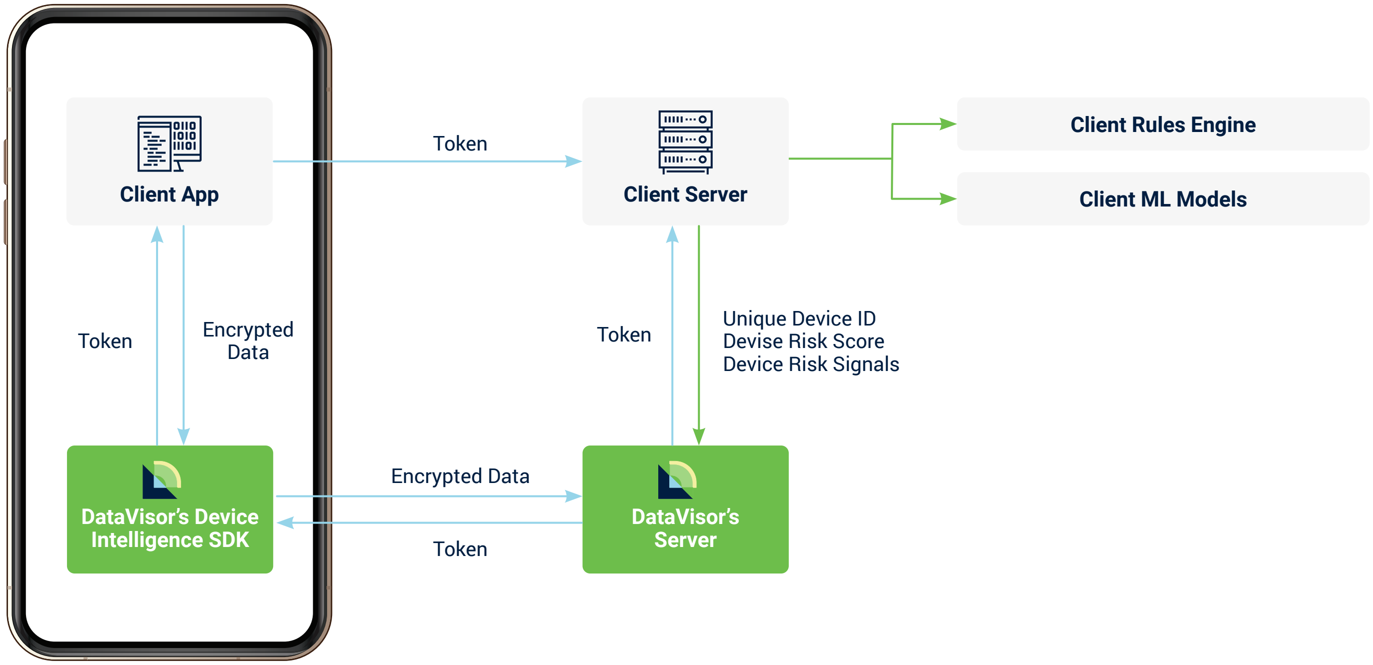
When used in conjunction with other DataVisor machine learning solutions, the device intelligence solution empowers clients to uncover known and unknown threats and attacks early and take action with confidence.



3 Device Intelligence: How It Works

DataVisor's device intelligence SDK seamlessly integrates with client apps to collect a variety of fields from user devices in real time. With each device, the solution uses advanced machine learning and encryption to assign a unique and consistent Device ID that never changes, even if the user resets the device or deletes apps.

A unique encryption key per device is sent to DataVisor's device intelligence servers to keep device data secure. These keys cannot be found with debugging nor do they exist in memory, disc, or network data.



4 Device Intelligence: Types of Device Manipulation Techniques Detected

Datavisor's device intelligence solution can be deployed across a number of industries and use cases to identify multiple types of mobile and web fraud that existing solutions cannot accommodate.

Common device manipulation techniques include:

Emulators

Emulators allow users to run software from a different device on your computer. Bad actors use emulators to control thousands of synthetic mobile devices simultaneously and in real time, which can result in a large-scale attack against a business. These attacks usually take the form of account takeovers, promotion abuse, fake account creation, and more.

Bots

Botnets are programmed to perform repetitive tasks on autopilot, allowing fraudsters to carry out activities in little time with little effort. They could perform 100+ attacks in seconds, which poses a significant threat to businesses.

App Cloners

App cloners can be leveraged to install hundreds of the same mobile app on one device, which means fraudsters can have multiple accounts of the same app on a single device. This allows them to easily manage hundreds of accounts and commit massive-scale fraud on a single app.

Repackaged Apps

Fraudsters can manipulate legitimate apps with malicious code before distributing it to unsuspecting victims. These repackaged apps can then be used to steal user data, deactivate anti-malware, or other activities that can pose a risk to the end-user and a business's reputation.

Jailbroken and Rooted Devices

Jailbreaking an iOS device or rooting an Android device is the first step toward turning a device into a potential weapon of fraud. Once past this step, fraudsters can install emulators or other destructive tools. Detecting devices that are capable of committing fraud can help companies prevent users with these devices from moving forward.

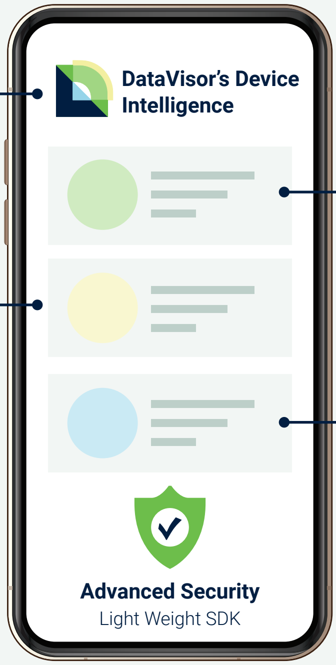
Hooked Devices

Hooked devices fly under most fraud detection radars because their parameters can be altered to avoid observation. For example, a hooked device can appear to be multiple devices, which makes it harder to trace its activities.

5 Device Intelligence: Features and Functions

Device intelligence technology helps organizations combat some of the biggest pain points of mobile and web fraud detection and prevention. Features and functions include:

DataVisor Device Intelligence: Leveraging Device Intelligence to Defeat Threats From Mobile and Web



Consistent Device ID

Provide persistent device IDs no matter how attackers manipulate or reset the mobile devices powered by machine learning engine

Compromised Device Detection

Detect emulators, root, jailbreak, botnets, VPNs, app cloners, repackaged apps, even for the latest versions of the attack tools

Advanced Device Signal

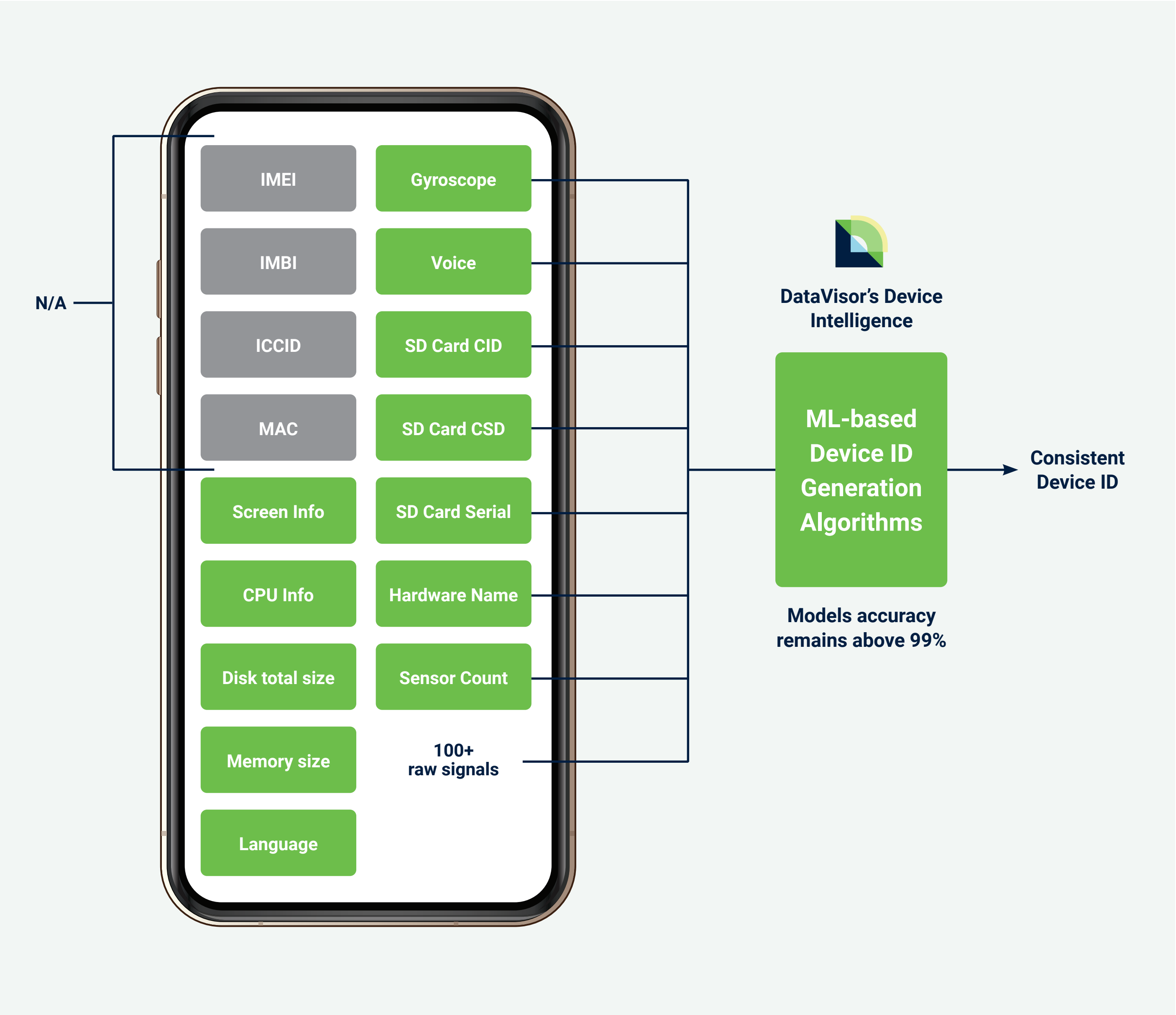
Deliver risk signals – such as the numbers of app re-installations – to make better decisions.

Accurate Device Risk Score

Provide accurate device risk score by holistically analyzing diverse fields and signals, empowering businesses to take immediate and confident actions

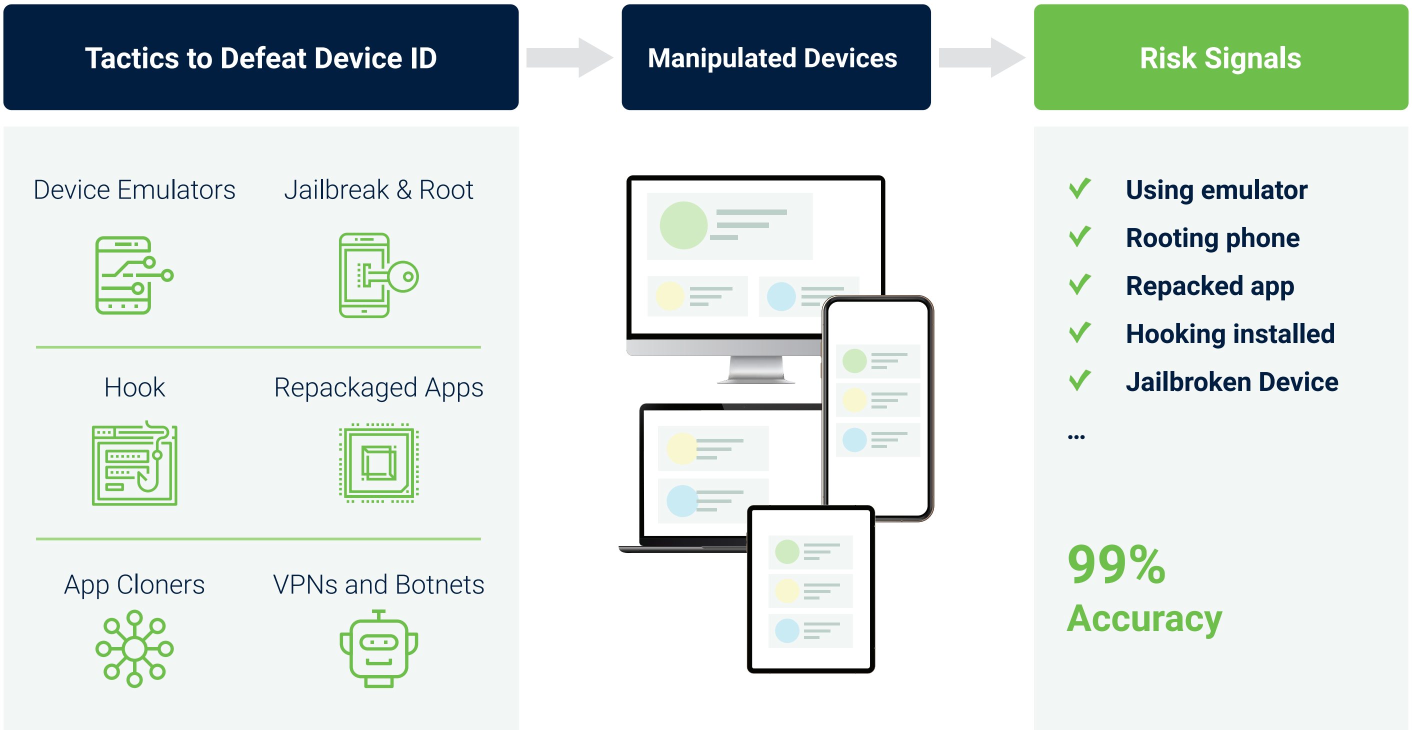
1. Unique, Consistent Device IDs

DataVisor's device intelligence solution generates consistent device IDs even when attackers manipulate or reset devices multiple times or when IMEA and IMEI are missing. It can even detect bad actors abusing the new Macbooks with MI chips. It leverages advanced machine learning algorithms and takes a holistic approach to analyze abnormal signals and extensive device information. In other words, the device ID remains the same no matter which apps are uninstalled or which device parameters are changed.



2. Advanced Device Manipulation Detection

Advanced attackers use techniques such as emulators, botnets, app cloners, repackaged apps, VPNs, and other tools, all of which can be captured by DataVisor's device intelligence solution. The solution makes accurate distinctions between trusted devices and those evidencing signs of manipulated devices.



Tactics to Defeat Device ID

Device Emulators

Jailbreak & Root

Hook

Repackaged Apps

App Cloners

VPNs and Botnets

Manipulated Devices

Risk Signals

- ✓ **Using emulator**
- ✓ **Rooting phone**
- ✓ **Repacked app**
- ✓ **Hooking installed**
- ✓ **Jailbroken Device**

...

99%
Accuracy

3. Accurate Device Signals and Scores

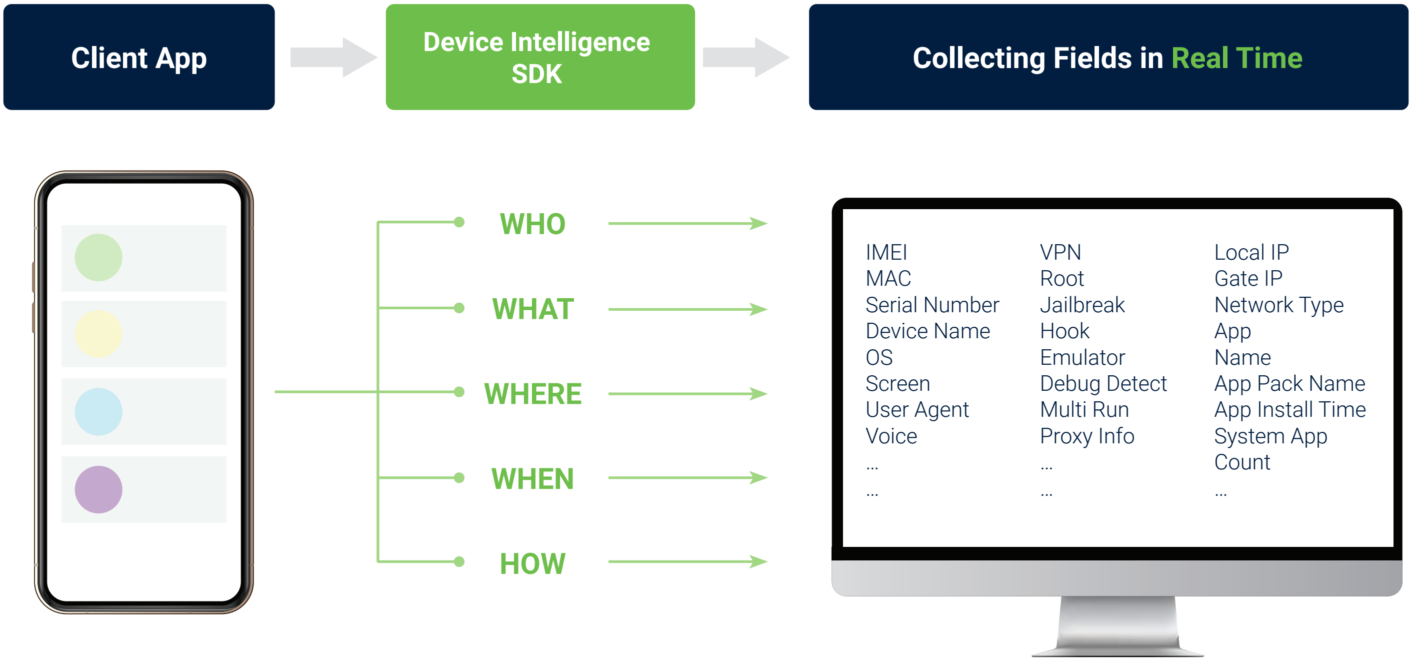
Manipulated devices send out a number of risk "signals" that indicate potential fraud. These signals help companies identify whether a device might be jailbroken, emulated, or otherwise manipulated so that fraud teams can make better and more accurate decisions. Depending on the signals, each device will also be assigned a score powered by machine learning so rapid decisions can be made based on how suspicious the activity appears.

Device score powered by ML

Device ages from global customers

4. Real-Time Device Intelligence and Event Tracking

DataVisor reviews device intelligence in real time to streamline decision-making for fraud teams. Collect accurate and extensive intelligence from Android and iOS devices and web pages, including data from more than 100 fields related to device information, operating systems, network, timestamp, languages, user agents, and more. What's more, the solution also protects consumer privacy by not collecting Personal Identifying Information (PII) data.



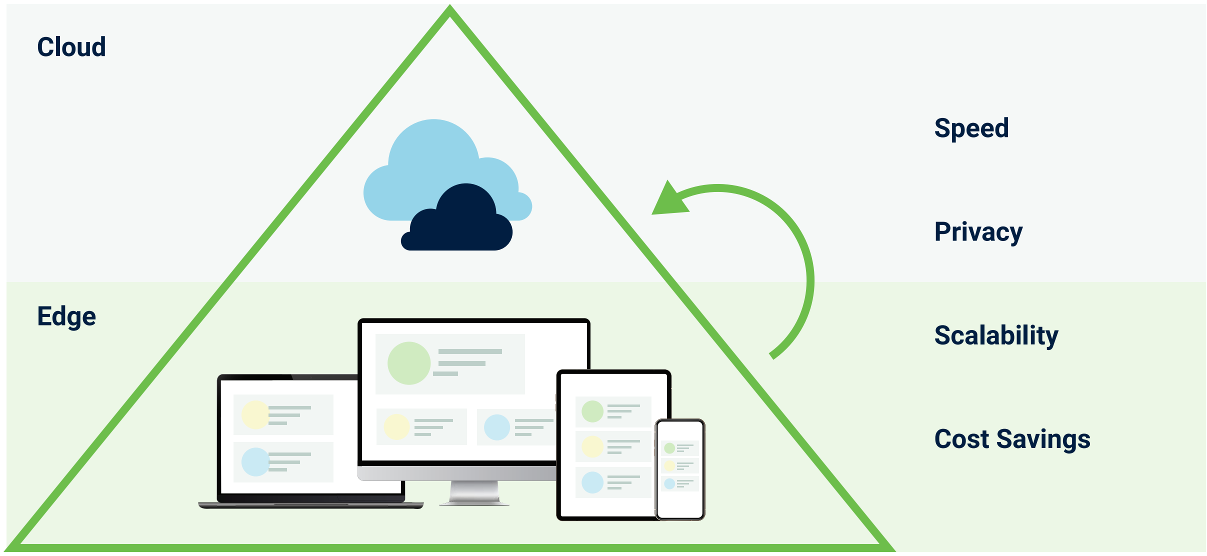
IMEI
MAC
Serial Number
Device Name
OS
Screen
User Agent
Voice
...
...

VPN
Root
Jailbreak
Hook
Emulator
Debug Detect
Multi Run
Proxy Info
...
...

Local IP
Gate IP
Network Type
App
Name
App Pack Name
App Install Time
System App
Count
...

5. Edge Computing

Mobile fraud detection need not be a drain on resources. To enhance the performance of the solution and ensure resource optimization, DataVisor's device intelligence solution leverages edge computing. Allowing data from connected devices to be analyzed at the edge of the network before being sent to the cloud or to a data center eliminates latency, improves network performance, reduces the risk to customer data, improves scalability, and results in cost savings overall.



6. Data Security

DataVisor's device intelligence solution uses best-in-class encryption algorithms and digital signature to prevent hijacking or tampering of data. Fully secured data transmission means fraudsters cannot copy, sync, or transfer the data for offline analysis. A unique encryption key for each device provides enhanced security.

Other Solutions	DataVisor Solutions
• **Basic Encryption** Need only a few days for fraudsters to break the encryption	• **Best-in-Class Encryption** Leverage advanced encryption algorithms to achieve the same or better performance as AES256-CBC
• **Easy to Find Plaintext Key** Easy to use debug to find plaintext key	• **No Plaintext Encryption Key** Keys cannot be founf using debugging, and keys do not exist in memory, disc or network
• **Data Hijacking & Tampering** Vulnerable to data hijacking and tampering due to weak encryption	• **Stop Data Hijacking / Tampering** Leverage advanced encryption and digital signature to secure data from being hijacked or tampered
• **Insecure Data Transmission** Easy for fraudsters to transfer data at large scale and analyze data offline	• **Protect Data Transmission** Protect data from being copied, synced or transferred, and stop fraudsters from analyzing data offline
• **One Key for All Devices** If one device is compromised, then all other devices are at risk	• **Unique Encryption Key Per Device** Provide advanced security for all other devices – even when fraudsters compromise a few devices

6 DataVisor Device Intelligence: Popular Use Cases

Today’s business environment is increasingly online and mobile, which ultimately means a greater variety of targets for fraudsters. DataVisor address multiple industries’ needs across a myriad of use cases, including the following:

Financial Institutions

Any industry where the exchange of monetary goods and services is the focus is a prime target for fraudsters. Device intelligence can help to curb application fraud, third party fraud, synthetic identity fraud, transaction fraud, and account takeovers by flagging suspicious devices and stopping transactions and applications.

eCommerce Platforms

Similar to the financial industry, eCommerce companies are high stakes in the fraud arena. Identifying mass fraud attacks by using device intelligence can prevent promotion abuse, chargebacks, account takeovers, and payment fraud.

Social Media

Social media platforms have come under fire in recent years due to the number of fake users that engage with real users. Device intelligence can help to mitigate the effects of mass registration, spam accounts and postings, and account takeovers of authentic users.

7 Simple Integration for Powerful Protection

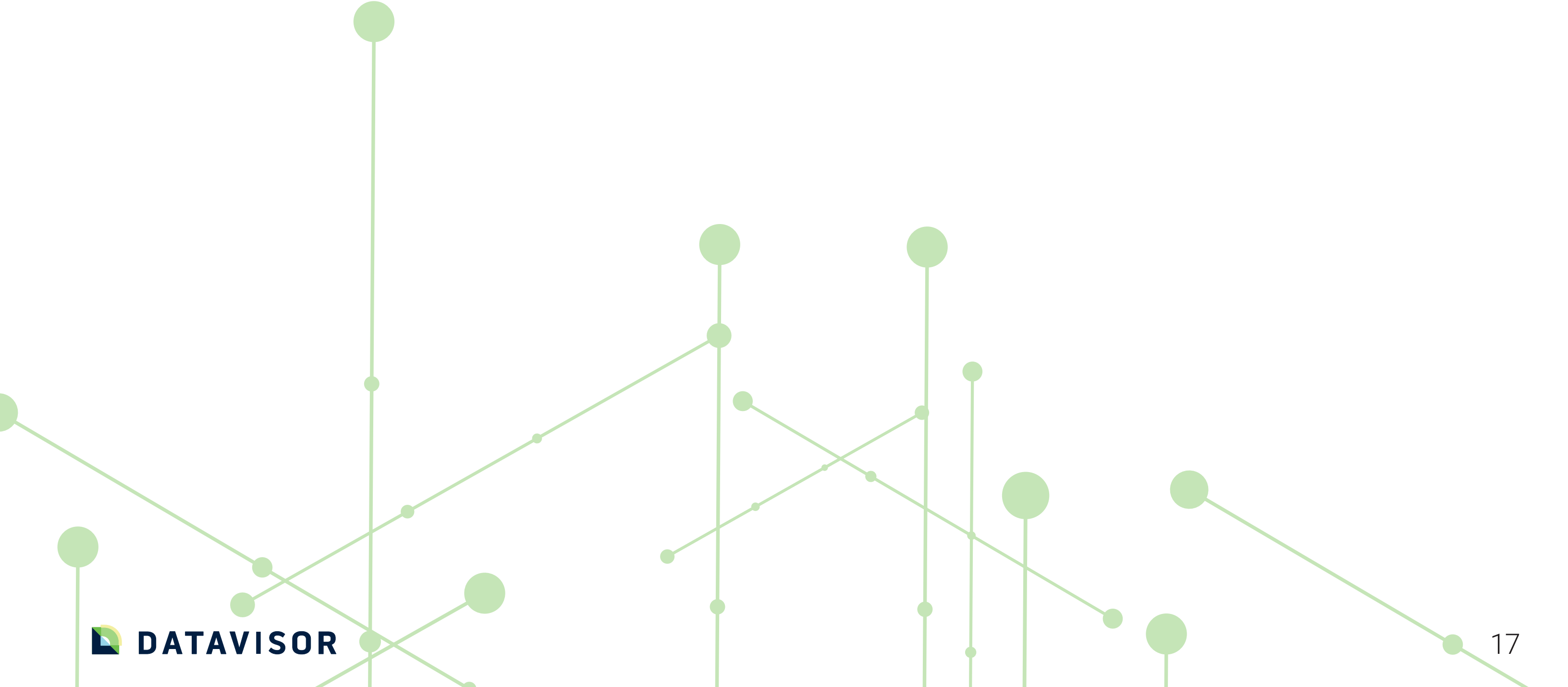
DataVisor's device intelligence infrastructure allows users to quickly deploy it and start seeing an **ROI in as little as two weeks**. The integration supports iOS apps, Android apps, and web browsers, offering 360-degree protection to mitigate fast-evolving threats.

If you are using other DataVisor solutions, our device intelligence features work seamlessly with these tools.

Our integration process is simple and straightforward:

1. Embed the DataVisor SDK to your Apple/Android app or home page.
2. Initialize the app to send device information to our server and retrieve the device token.
3. Query the DataVisor device intelligence server WebAPI to obtain device signals.
4. Integrate the device signals with your solutions to elevate detection capabilities.

Throughout the integration process, we offer dedicated 24/7 support from our technical account managers. Get help via email, Slack, Workspace, and the DataVisor support portal. Our team provides comprehensive training and continuing performance monitoring to ensure you get the most from your solutions.



8 Combining the Power of Device Intelligence with Machine Learning

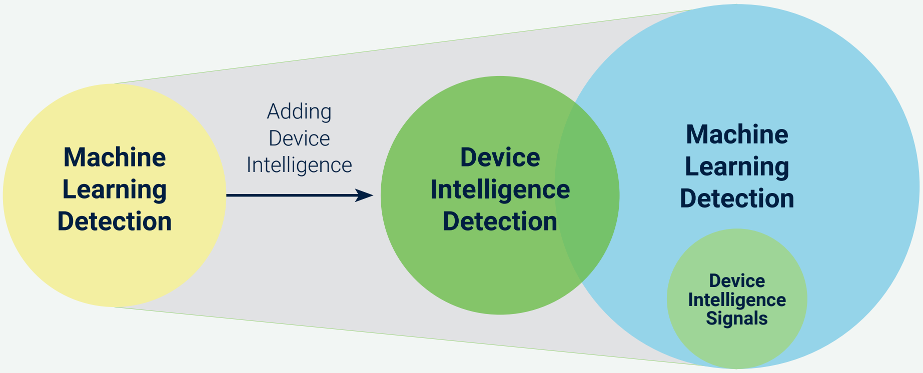
The device intelligence solution is one of many products developed by DataVisor and enhances DataVisor's unsupervised machine learning model. Together, the two work to provide high-quality, reliable data and detect more fraud with greater accuracy.

CASE STUDY – How DataVisor Device Intelligence Signals Enhanced Fraud Detection

- A **Leading E-Commerce Platform** has been integrating with DataVisor Machine Learning since 2018 for promo abuse use case.
- **Fraud patters detected by DataVisor Machine Learning** suggested more and more sophisticated device manipulation techniques.
- Existing device ID solution could not catch up to provide **persistent device IDs or useful signals**.

DataVisor Machine Learning

DataVisor Device Intelligence + DataVisor Machine Learning


Machine Learning Detection
Adding Device Intelligence
Device Intelligence Detection
Machine Learning Detection
Device Intelligence Signals

62%

Detection uplift for DataVisor Machine Learning after incorporating DataVisor Device Intelligence signals

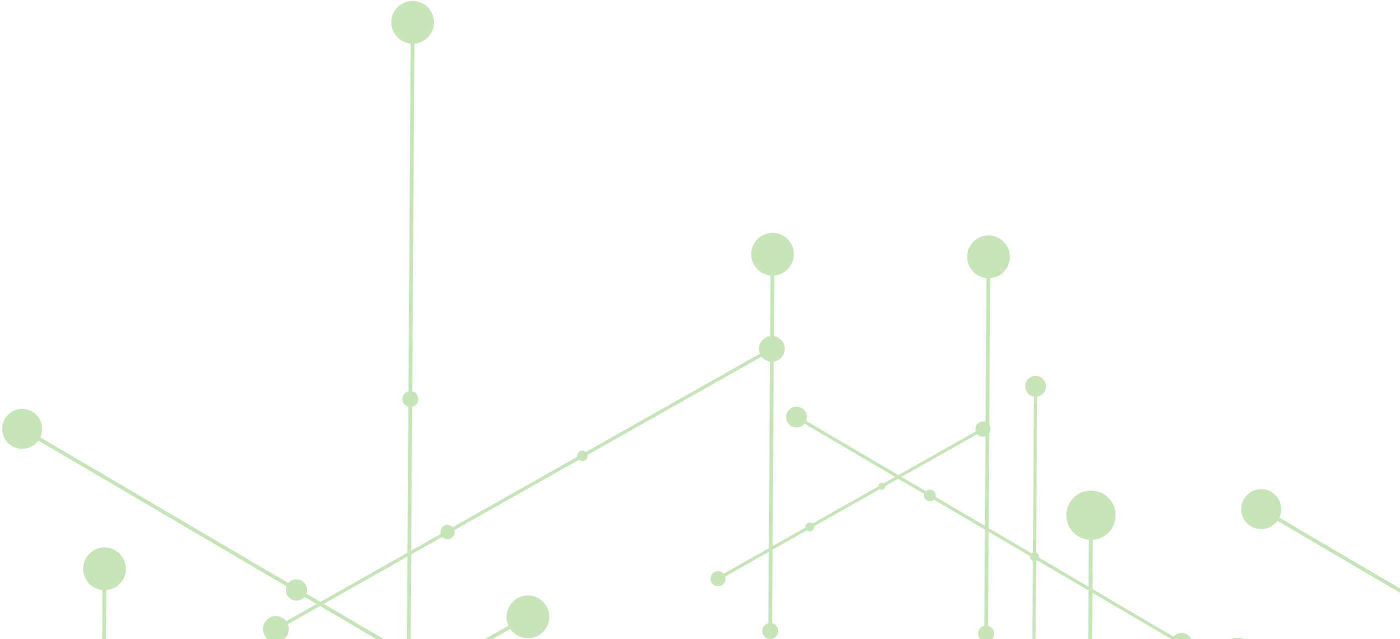
28%

Additional fraud captured by only using DataVisor Device Intelligence signals

In a recent case study, we examined a leading eCommerce platform and their investigation into promotion abuse. The customer found that fraudsters were running multiple accounts simultaneously on a single device. Existing device ID tools didn't provide enough useful signals and couldn't catch up to quickly evolving attacks.

After integrating device intelligence, the unique Device ID remained the same no matter how the fraudsters evolved their attacks. Adding device intelligence to their current ML-powered DataVisor solutions resulted in a 62% detection uplift and 28% additional fraud captured using device intelligence signals.

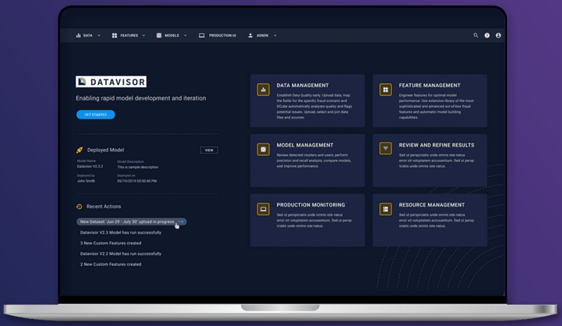
Discover more about DataVisor's device intelligence mobile fraud solution when you, **request a demo**.



Experience proactive AI-powered fraud prevention today.

GET A DEMO

DATAVISOR



DATAVISOR

Enabling rapid model development and iteration

Deployed Model

Model Name: Datavisor V2.3.3
Model Description: This is sample description
Deployed by: John Smith
Deployed on: 05/19/2019 03:30:40 PM

Recent Actions

New Dataset 'Jun 29 - July 30' upload in progress
Datavisor V2.3 Model has run successfully
3 New Custom Features created
Datavisor V2.2 Model has run successfully
2 New Custom Features created

DATA MANAGEMENT
Establish Data Quality early. Upload data, map the fields for the specific fraud scenario and DCube automatically analyzes quality and flags potential issues. Upload, select and join data files and sources.

FEATURE MANAGEMENT
Engineer features for optimal model performance. Use extensive library of the most sophisticated and advanced out-of-box fraud features and automatic model building capabilities.

MODEL MANAGEMENT
Review detected clusters and users, perform precision and recall analysis, compare models, and improve performance.

REVIEW AND REFINE RESULTS
Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium. Sed ut persp iciatis unde omnis iste natus.

PRODUCTION MONITORING
Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium. Sed ut persp iciatis unde omnis iste natus.

RESOURCE MANAGEMENT
Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium. Sed ut persp iciatis unde omnis iste natus.

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

DATAVISOR