Cleafy

Does your online fraud management system tick every box?

The 5 key considerations to fight online banking fraud efficiently

Checklist

How to understand if your fraud management system is the right one

Financial fraud attacks have notably increased in recent times, accelerated by a new push towards digitalization observed during Covid19 pandemic. Together with the **development of new and more efficient technologies** comes the fraudsters' ability to elaborate **more sophisticated means to attack financial systems** and breach into highly protected databases.

Banks and financial institutions need to **increase the level of protection** of their client's data and improve the way they manage internal processes and fraud management systems. Now more than ever, when choosing a digital financial service, **customers need to feel safe** and to complete activities across devices in the fastest and easiest possible way.

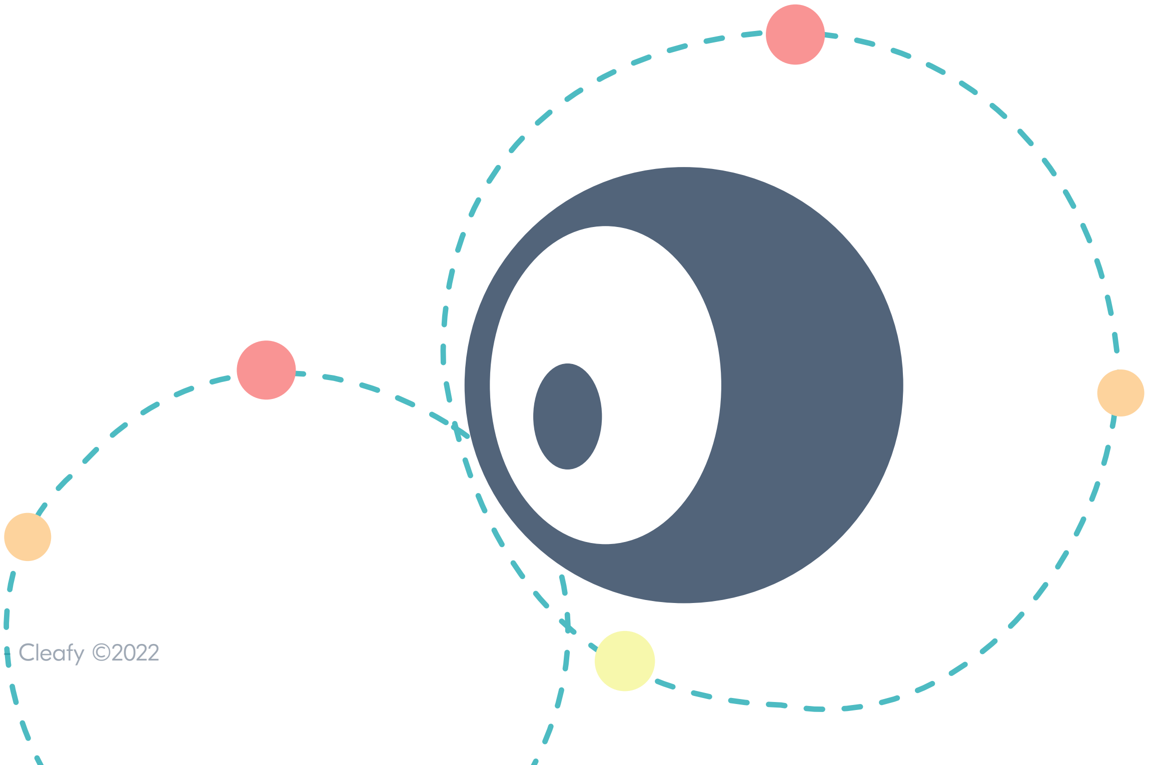
Managing online fraud doesn't have to be a headache, though. To make sure to safeguard your business and **your people's mental health**, it is essential to choose the right fraud management solution. Which is to say the one that **combines all the key features** to monitor and stop fraud quickly and efficiently, **reduces customers friction** and **ensures the best online user experience**.

See all details of users' sessions 1

Seeing all details is important because it allows you to shift from blocking all to **responding with surgical precision** and **setting up the best response** for each micro-scenario.

The right fraud management system provides you with **atomic visibility** that goes behind risk scores, as they don't tell you enough about each session. Moreover, atomic visibility speeds up the process of **identifying new pattern of attacks** that are new and still not classified, which also remove the need to rely on external classifications.

How much detail of each user session can you actually see?



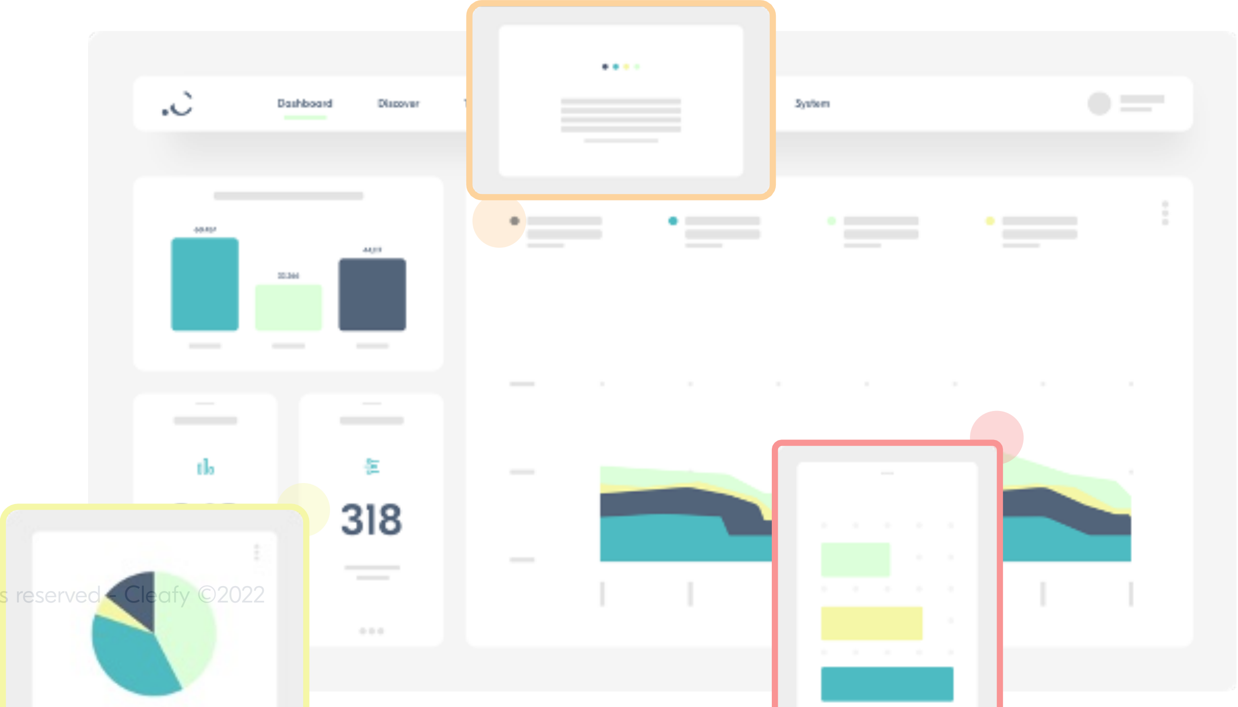
Monitor & respond in real-time 2

Today, customers expect to get things done within a few seconds. If the detection tool doesn't respond instantly it could:

- **Slow down your customers' activity**, making them wait impatiently
- **Force the app to block the activity**, causing frustration and anger
- **Force the app to finalize the activity**, possibly giving the green light to a fraudster

The right fraud management system provides you with an accurate and instant response, ensuring **smooth usability** of your digital services and **minimizing the risk of fraud**. The optimal response time is <300ms.

Do you know how long your fraud management system takes to respond?



Detect anomalies quickly

3

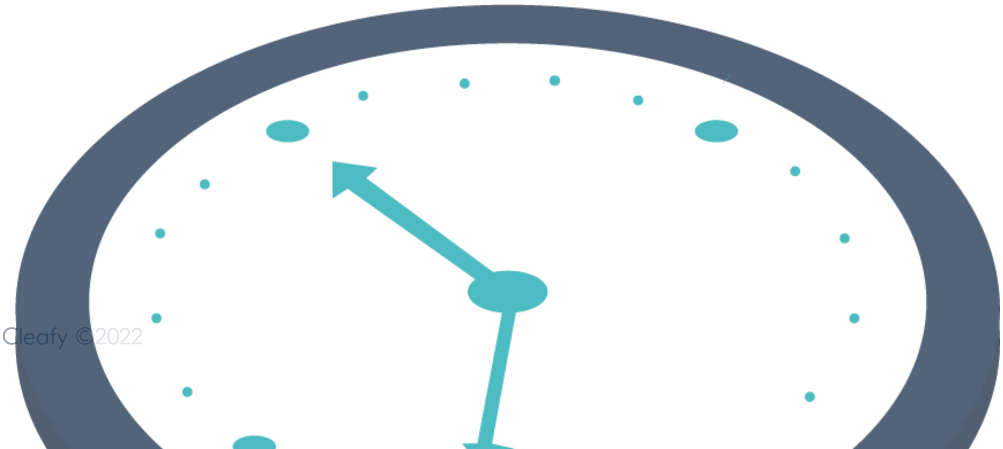
It can take weeks to understand where to focus on when looking for new suspicious patterns. To avoid giving fraudsters the time to hit, it's important for your analysts to focus fast on what really matters.

The right technology is the one that combines **all key detection capabilities to**:

- **Highlight potential malicious activities** via Multidimensional Analysis of all data across your channels.
- **Verify the user identity** via **Behavioral Biometrics** and Behavioral Analysis.
- **Assess the device integrity** via Malware and Bot Detection.
- **Check all transactions** via Transactional Risk Analysis.

The right fraud management system helps you find what's off in a matter of minutes.

How long does it take you to find new anomalies on your digital channels?



Set up appropiate response to threats easily

4

Often, configuring and testing all the integrations and conditions to set up a response for each scenario can be a headache. And too often this leads to a tight **trade-off between high friction or high-risk**.

To ensure the **safest and smoothest experience** for your customers it is important to set up the best response and automate it.

The right technology allows you to easily set up **smart rules** to do that, so that you can make sure the right thing is done, always. Even when your digital channels are under a massive attack.

The right fraud management system helps you set up your **security posture** with no headache and gives you more time to **focus on developing your product**.

How easy it is for you to set up appropriate responses to threats?

Integrate Tailored Threat Intelligence 5

Monitoring fraudsters' move is a stressful and time-consuming task. A Tailored Threat Intelligence team can do the heavy-lifting job by **identifying and classifying all the possible threats** that target your systems.

Integrating a Tailored Threat Intelligence support with the right technology eases your processes and relieve your team from stress, **improving the efficiency** of your fraud management.

How easy it is for your fraud analysts to keep track of what's happening in the cyberworld?

All-in-one with Cleafy

Finding the right fraud management system is not easy. Neither fighting fraud.

That's why, at Cleafy, we carefully developed a **all-in-one platform** that combines multiple tools to satisfy multiple needs at once. Easily integrable with existing security systems you might have already in place, Cleafy platform is **built in modules** that can work independently and are chosen with our fraud experts according to your business objectives and technical requirements.

Our **white-box approach** allows the most granular visibility of what's happening across your digital channels, unlocking the possibility to classify specific micro-patterns as threats. This translates into a more precise response and less friction for genuine users.

By constantly innovating and introducing improvements to our platform, we guarantee **safety, control, and smooth usability** to both you and your customers.

Cleafy's unique differentiators

- **Continuous real-time passive monitoring**
covering the entire user journey, even before the log-in
- **Multi-entity analysis**
including device integrity, transactional and user's identity
- **White-box complete visibility**
to see all conceivable events and data beyond risk scores
- **Cross-channel risk propagation**
via events real-time and historical correlation
- **User prediction extended capabilities**
based on proprietary ML behavioral analysis, and behavioral biometrics
- **Tailored banking threat intelligence** (C | Labs)
Actionable TI from your & your peers' traffic, delivering fresh data and threats
- **Deterministic 0-day malware detection**
via proprietary full content integrity check
- **Smart rules engine for adaptive response at scale**
To automate adaptive responses based on real threat patterns

Interested in learning more?

Get in touch

If you are interested in learning more about our Cleafy solution you can **contact us** or **book a 15 minutes call** with our sales representatives. No strings attached.

About Cleafy

We are a team of fraud hunters, cybersecurity experts, data scientists, and software engineers that since 2014 share the same dream: make technology a safer place.

Every day, we work side by side with our customers to help them safely navigate digital opportunities, while growing their business. And we do it with passion, determination, and constant curiosity about the unexpected.

Our purpose is to make people's life easier and free from the threats hidden in the digital ecosystem.

That's why we designed a real-time technology that enables financial institutions' fraud management teams to detect and prevent financial fraud across all digital channels, while ensuring a safe and seamless experience for the end-users.

Recognized as a market leader by industry analysts, today we protect over 60M+ users of top-tier retail and corporate banks against financial online fraud.

cleafy.com