



**Making technology
a safer place**

Fraud Management Solution
for Banks and Financial Institutions

2021

Table of contents

/ 1

Introduction p. 4

/ 2

A new era for banks and financial institutions security p. 6

Demand for omnichannel customer experience p. 8

Rising volume and complexity of online attacks p. 11

Compliance with regulations p. 14

/ 3

Limits of the traditional fraud management approach p. 15

/ 4

Cleafy: changing the game in online fraud management p. 22

Who we are and why choose us p. 23

How do we help banks and financial institutions p. 26

Our fraud management solution p. 29

Table of contents

/ 5

A sneak peek of the Cleafy platform p. 33

Our platform, your safety p. 35

Know your user p. 35

Stay one step ahead p. 40

Move fast and precisely p. 42

SaaS Deployment p. 44

/ 6

Our customers' voice p. 45

/ 7

Success Story: Digital banking made safe and seamless p. 47

/ 8

Cleafy: Your freedom to look ahead p. 54

Introduction

Introduction

Financial fraud attacks have notably increased in recent times, accelerated by a new push towards digitalization observed during Covid19 pandemic.

According to BusinessWire, only in 2020 74% of Financial Institutions experienced a rise in cybercrime, of which 56% led to an associated increase of financial losses. ¹

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 way possible.

Security and risk management leaders must ensure an **effective, fast and reliable fraud management management system** to prevent attacks from a variety of worldwide automated and human vectors.

In this document, you'll understand what Cleafy is and how it will help you protect your users from online financial fraud.

¹ BusinessWire "COVID Cyber Crime: 74% of Financial Institutions Experience Significant Spike in Threats Linked To COVID-19"

*A new era for
banks and financial
institutions security*

Banks and financial institutions are facing a fast-changing landscape characterized by three main factors:

1. Demand for omnichannel customer experience
2. Rising volume and complexity of online attacks
3. Compliance with regulations

Let's have a look at each of them.

Demand for omni-channel customer experience

Only a decade ago, **digital banking** was perceived as a modern nice-to-have, but its acceptance came about quickly. The development of online retailers, music streaming services, taxi-hailing apps, and instant messaging has considerably contributed to changing customers' expectations of digital banking and financial services.

Today, customers demand services that are available anytime, anywhere.

In particular, the **digital payments market** is expected to grow about 20% CAGR by 2026, reaching \$175.8 billion over the forecast period. This trend is facilitated by the growing number of mobile devices users across new segments of the global population. ²

² "Global Digital Payment Market By Component, By Deployment Type, By Enterprise Size, By End User, By Region, Industry Analysis and Forecast 2020 - 2026", ResearchAndMarkets.com report (2021)



Big tech companies and new players in the fintech space are expanding their market share above any prediction as they are able to offer **innovative and smart services** to their clients.

Ensuring instant services and frictionless user experiences across multiple digital channels has become essential to survive in a crowded market.

Where does this leave banks and financial institutions?

The service level they provided yesterday no longer meets the expectations customers have today. They need to step up and **make their services easier, more available, and more personal** to please customers and retain their business. Central to meeting customers' expectations is the idea of **providing an omnichannel digital experience.**

**The run to digitalization and innovation brings
with it a new level of risk exposure.
A risk that must be kept under control.**

Rising volume and complexity of online attacks

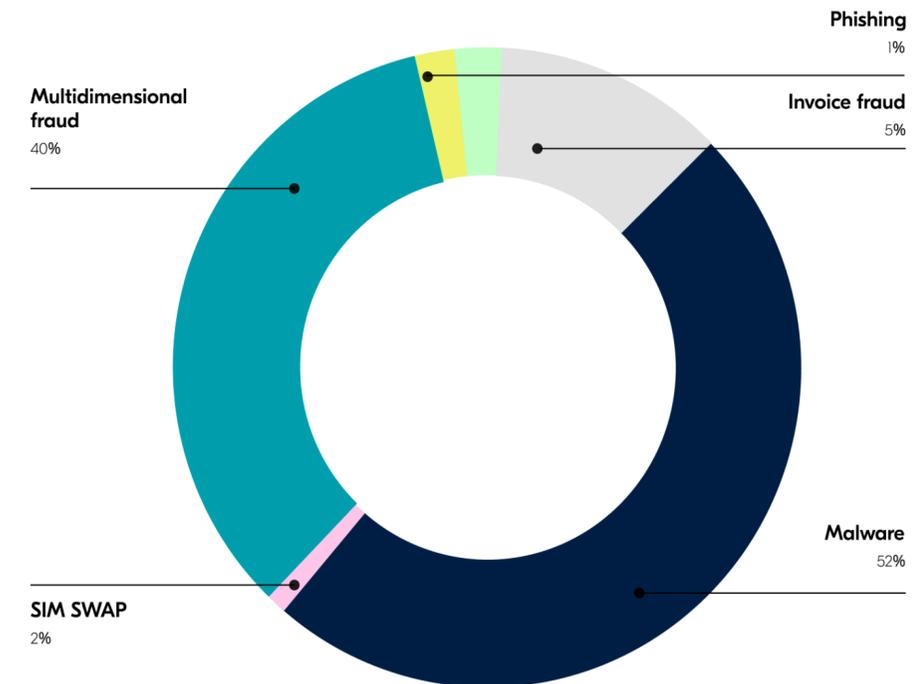
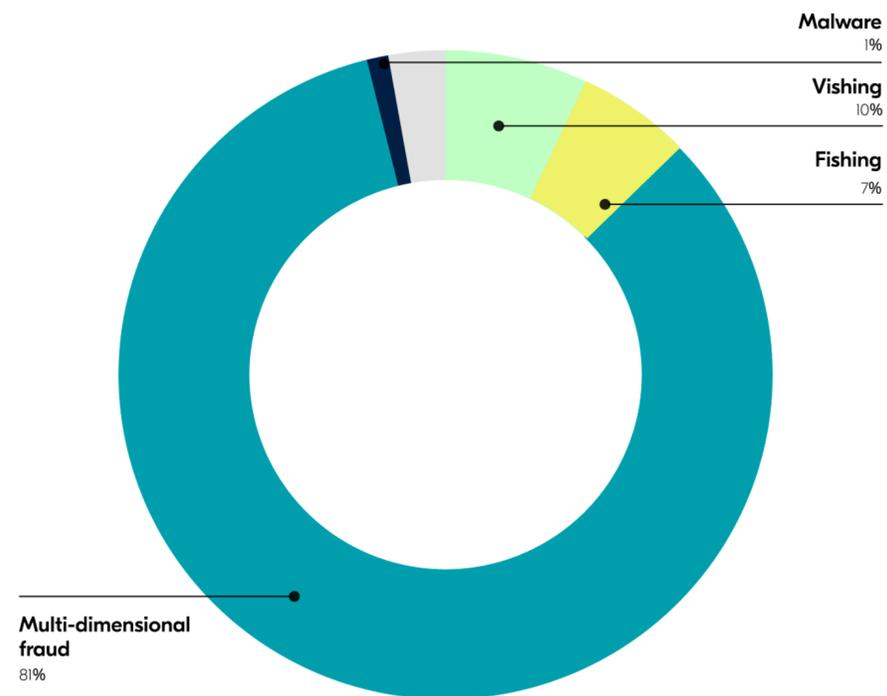
The volume of attacks to financial online services is also growing fast (3.6x year over year)³, for an estimated 1M users attacked across the globe in 2021. The **increase of instant payments** is expected to further exacerbate the issue.

Fraudsters can now leverage **customizable toolkits** that have become easily available on the black market. This is how they craft **targeted malware** and can establish botnets of infected computers to launch and control campaigns of attacks that strike at scale.

³ "Internet Threat Security Report", Symantec (2015, 2017, 2018)

At Cleafy we adopted the term **multi-dimensional** to characterize the new generation of fraud attack strategies, a combination of ultra-tailored malware and highly structured social engineering techniques. As these techniques keep evolving, it becomes extremely challenging to detect attacks through the

traditional approach of many fraud management departments. This usually includes multiple teams working in silos on multiple separated solutions⁴. We clearly see the limitation of this way of working when it comes to fraud detection and prevention capabilities.



Mixed social engineering and malware attacks up to 81% retail banking (mobile channel), 40% corporate banking.

⁴ CERTFin report: Online Fraud in Banking, May 2021

A new approach that guarantees considerably more granular detection and response is needed.

Compliance with regulations

When assessing the risk of a transaction, compliance regulations require the identification of **signs of malware infection on devices** to minimize the risks of mistaken or fraudulent transactions.

To protect customers, banks and Payment Service Providers (PSPs) operating in Europe are required to comply with Payment Services Directive regulations (PSD2) issued by the European Banking Authority (EBA).

PSD2 requires the adoption of Transactional Risk Analysis (TRA) mechanisms to detect in real-time several risk factors in a user session and thus minimize the risk of fraud.

Achieving PSD2 compliance with traditional fraud management solutions presents several challenges, including:

- **missing malware detection capabilities** for detecting signs of malware infection, either during the authentication phase or in any other phase;
- **required application changes** that impact application development and affect the ability to deliver new business functions;
- **long implementation time and huge implementation effort** caused by solution complexity and available integration approach.

Moreover, banks and financial institutions need to ensure that their fraud management system complies with **privacy and data management regulations** (e.g. GDPR in Europe, EPPA in California, LGPD in Brazil) to guarantee the correct use of customers' data.

The cost of not respecting these requirements can be dire in terms of penalties and brand reputation.

Limits of the traditional fraud management approach

The traditional way to fight online fraud is based on a **serial assessment approach**. This implies relying on **siloed solutions that work separately** to assess the risk of each session.

When using multiple tools, across different vendors, and through different channels, the lack of interaction among these tools increases the chances to create an incomplete picture.

This usually results in either the block of a genuine session or, worse, the failure to detect a serious threat.



The traditional fraud management approach leads to:

High Risk and High Friction scenario

Too often we witnessed very strict security postures and yet too many successful attacks. The new threat landscape has made the trade-off between user friction and exposure to risk much tighter.

Slow attacks response

The presence of multiple tools and dashboards, together with the lack of critical visibility, require long investigations. Fraud management teams find it difficult to understand what's happening and respond quickly.

Unmanageable workload for fraud management teams

Without a deterministic classification of complex threats and automated adaptive responses, there are too many open cases for the fraud management team to investigate. The workload can quickly become hard to manage.

In these past years we have discovered that, before switching to Cleafy, our customers were facing six main limitations:

01.

Black-box risk scores

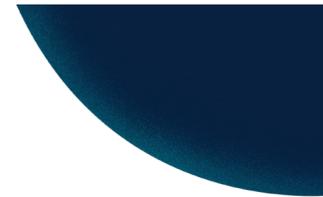
Risk scores are too high level, hide too much information, and work separately.



02.

Siloed views

Monitoring only the parts of the user journey that are considered critical, or at risk, cannot be effective against the new generation's online attacks.



03.

No cross-silos events correlation

Multiple high-level risk scores focused on a limited part of the story make it impossible to detect structured tailored attacks.



04.

Only near real-time

Too many fraud detection solutions can ensure only near real-time operativity. This is because of the way they integrate within the already present ecosystems.



05.

Generic Threat Intelligence

Only a few solutions on the market recognize the need to integrate threat intelligence data. The only way to define optimal threat responses is by adopting tailored threat intelligence.⁵

06.

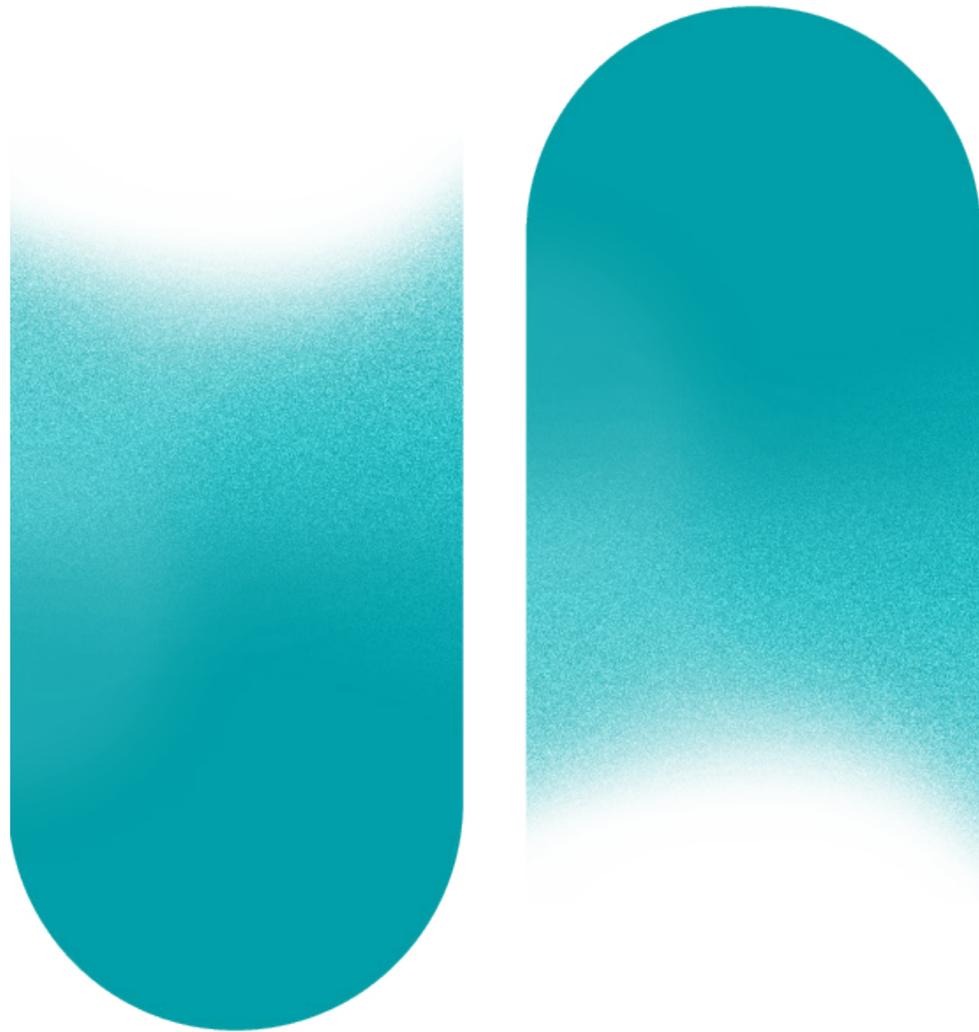
Response based on risk thresholds

In the traditional approach, a response is triggered when specific risk thresholds are met. Against new advanced threats, there is the need to respond to specific patterns, classified deterministically as threats.⁶



⁵ More on this at Chapter 4, paragraph “Clear all sessions”

⁶ More on this at Chapter 4, paragraph “Move fast and precisely”



On the other hand, an **approach based on parallel and multidimensional assessment** analyses all channels and touch-points at the same time and lets the system decide how to proceed according to the business security posture and compliance requirements set in advance.

This is how Cleafy platform works.

Limits of the traditional fraud management approach

Traditional approach

Black-box risk scores

Siloed views

No cross-silos events correlation

Only near real-time

Generic threat intelligence

Response based on risk thresholds

Cleafy approach

Granular end-to-end visibility

Multi-dimensional analysis

Continuous cross-channel events correlation

Actual real-time

Tailored Threat Intelligence

Dynamic response based on specific patterns

Cleafy: changing the game in online fraud management

Who we are and why choose us

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.**

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 technology that **identifies and prevents financial fraud in real-time**, while ensuring a safe and seamless experience for online users.

Recognized as the market leader by industry analysts, and selected vendor for Online Fraud Detection in the Gartner Market Guide 2018-2020, today **we protect over 60M+ users** of top-tier retail and corporate banks from financial online frauds.

And there's more...

Since we started, we have been driven by the awareness that knowledge and competence, algorithms and technology are not enough to achieve excellence.

There's the need for **human values** too.

Cleafy means:

Accountability

We take our own responsibility.
We never hide.

Responsiveness

We're here, as soon as you need us.

Proactivity

We know for sure that prevention
is better than cure.

Accuracy

We care about precision,
we admit no negligence.

Every day, we work side by side with our customers to help them **safely navigate the digital world, while growing their business**. And we do it with passion, determination, and constant curiosity about the unexpected. This is how we built **our expertise and deep understanding of financial fraud** together with long-term relationships based on **trust** and **transparency**.

By choosing Cleafy, you don't only choose a fraud management platform. You choose people who will do their best to keep you and your customers safe.

Anytime, anywhere.

How do we help banks and financial institutions

Cleafy helps banks and financial institutions to **scale up their fight against online fraud** thanks to its fully integrated platform that combines advanced fraud detection technologies with automated responses.

Our platform can be **easily integrated** with any component already deployed in the bank's ecosystem, without the need to change the protected applications.

Both your **business** and your **fraud management team** will achieve better results.



Main outcomes for the business

Faster business growth

Time to market for new digital products shrinks when security doesn't represent a bottleneck. Managing the risk means having more control to release new features and services.

Higher customers' satisfaction

The main outcome of an optimal security posture is to minimize friction for your users. Our platform triggers SCA⁷ mechanisms and other security procedures only when needed, allowing the smoothest user experience on your digital channels.

Full compliance with PSD2 and Open Banking regulations

Cleafy fully covers all regulation requirements, avoiding the risk of incurring costly penalties and reputational damages.

Respect for users' privacy

Our platform complies with the European GDPR policy and the American CCPA regulation to protect your users' data at every stage. This removes all headaches and guarantees trusted management of personal information.

Benefits for the fraud management team

The deployment of Cleafy's technology helps to achieve efficiency in everyday operations by decreasing the time to respond to attacks and reducing the workload and pressure on the fraud management team.

More effective detection of attacks

Our advanced technology enables atomic visibility of all your digital channels, allowing a precise detection of potential threats and granting tailored responses based on patterns identified.

Better product usability for the users

Users need smart, fast, and immediate access to their digital banking services. This is why we worked to enable a frictionless and safe user experience across channels.

Reduction of workload for the analysts

We believe that technology should make people's lives easier and help them to improve the way they work. Our product is designed to reduce the workload for the analysts and ease the burdens of their daily activity.

Our fraud management solution

Cleafy is the first solution to introduce **atomic detection and response** in online fraud prevention and to combine all the key features to detect, stop and hinder advanced threats in one central platform.

Know your users

With the most comprehensive and advanced set of fraud detection and identity verification technologies, you'll make sure only trusted users are let in.

Stay one step ahead

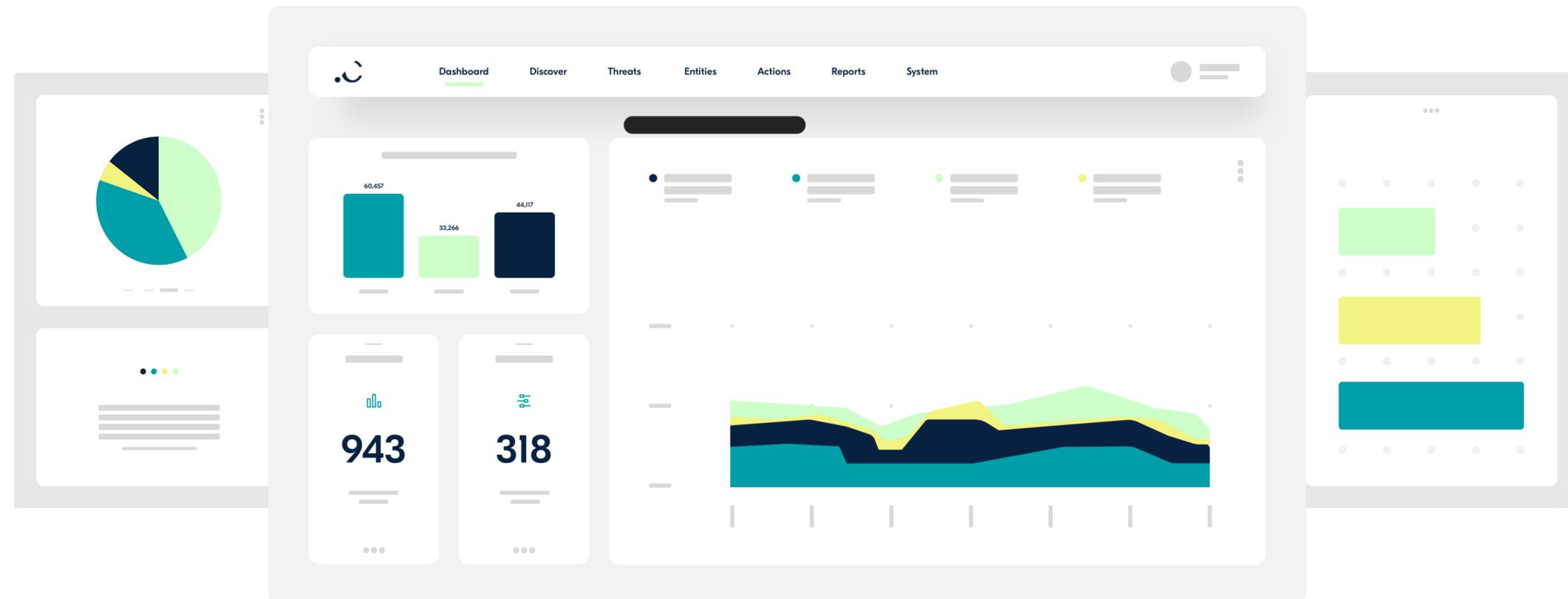
Thanks to our tailored up-to-date Threat Intelligence data and insights, you'll stay ahead of fraudsters' moves.

Move fast and precisely

By deploying adaptive response mechanisms based on patterns, we'll help you deal with any scenario in the best possible way.

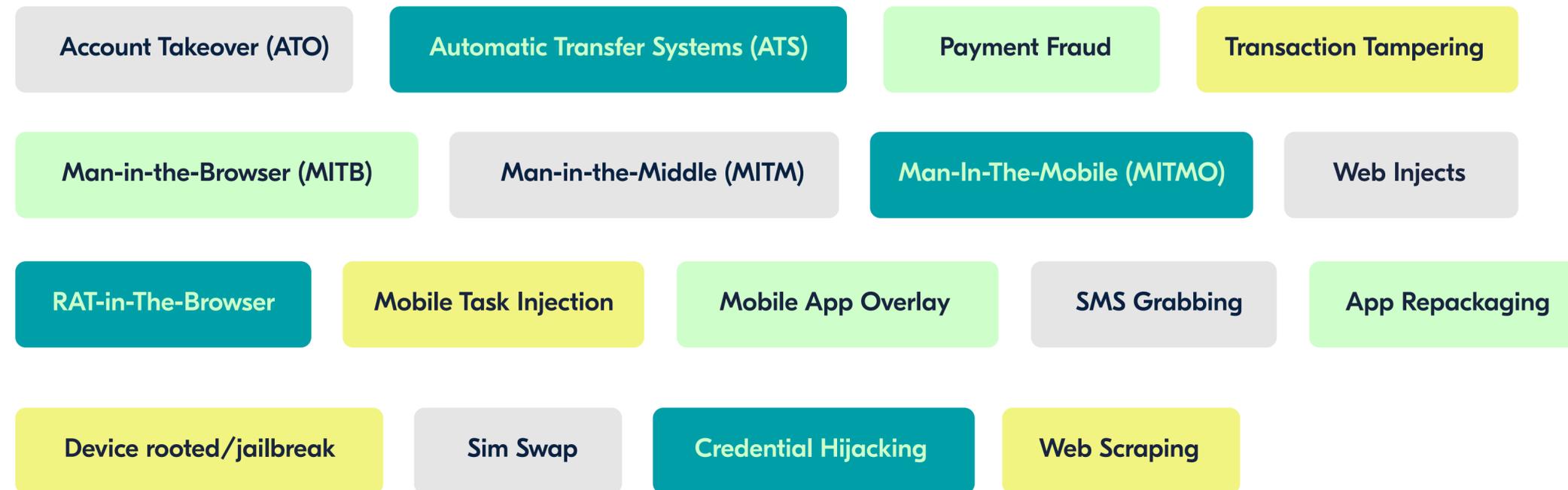
In line with the principles of the **CARTA approach**⁸, this technology combines multi-dimensional analysis with continuous cross-channel events correlation, ensuring actual real-time monitoring of all your systems.

From social engineering on your customers' accounts to automated attacks at API level, Cleafy detects and analyzes a wide variety of attack vectors used by fraudsters to steal credentials or manipulate transactions.



⁸ The Continuous Adaptive Risk and Trust Assessment (CARTA) approach was launched in 2019 by Gartner and requires continuous device visibility and automated control.

A representative list of fraud and attack techniques covered by Cleafy includes:



Cleafy's approach generates an optimal security posture: it maximises your systems' safety and the usability for the end-users.

A sneak peek of the Cleafy platform

While designing the platform we kept asking ourselves what we need to do, as fraud hunters, to do our job in the best way, and what we need to do, as humans, **to earn people's trust every day.**

The result is a solution 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 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.

Our platform, your safety

1. Know your users

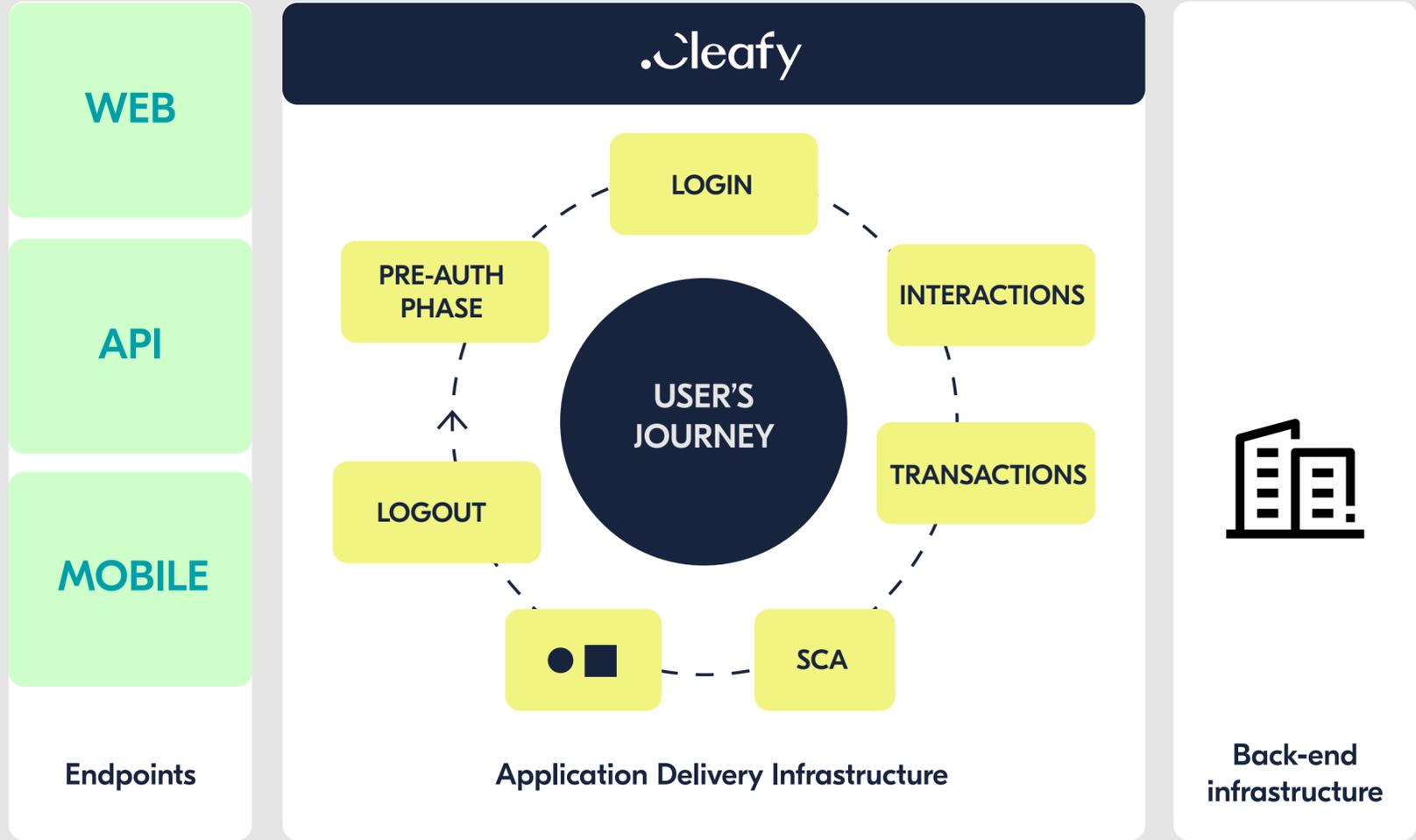
Cleafy's comprehensive and advanced identity verification technology facilitates the understanding of your users, avoiding the risk of letting fraudsters in and assuring a smooth and frictionless user experience for the trusted ones.

1.1 Atomic end-to-end visibility

Cleafy's patented technology makes it possible to see and analyze everything at an atomic level.

The continuous passive monitoring of all the application traffic ensures 100% visibility of what's happening in real-time on mobile, web, and API and extracts all information about your users' journey.

A sneak peek of the Cleafy platform



This distinguishes us from traditional online fraud management solutions that focus on one-time risk assessment on critical points (such as login or payment), losing part of additional data that could come during the process.

1.2 Multi-dimensional analysis

As fraud hunters we know the best way to make better and faster decisions is to be informed.

Fraudsters' advanced attacks happen on several dimensions, and Cleafy sees them all by gathering and analysing the broadest set of data on several dimensions.

With Cleafy you have all the information you need on one single platform.

Everything you need.
All in one place.



Transaction risk analysis.



Behavioral analysis.



Malware detection.



BOT detection.



Device telemetry.



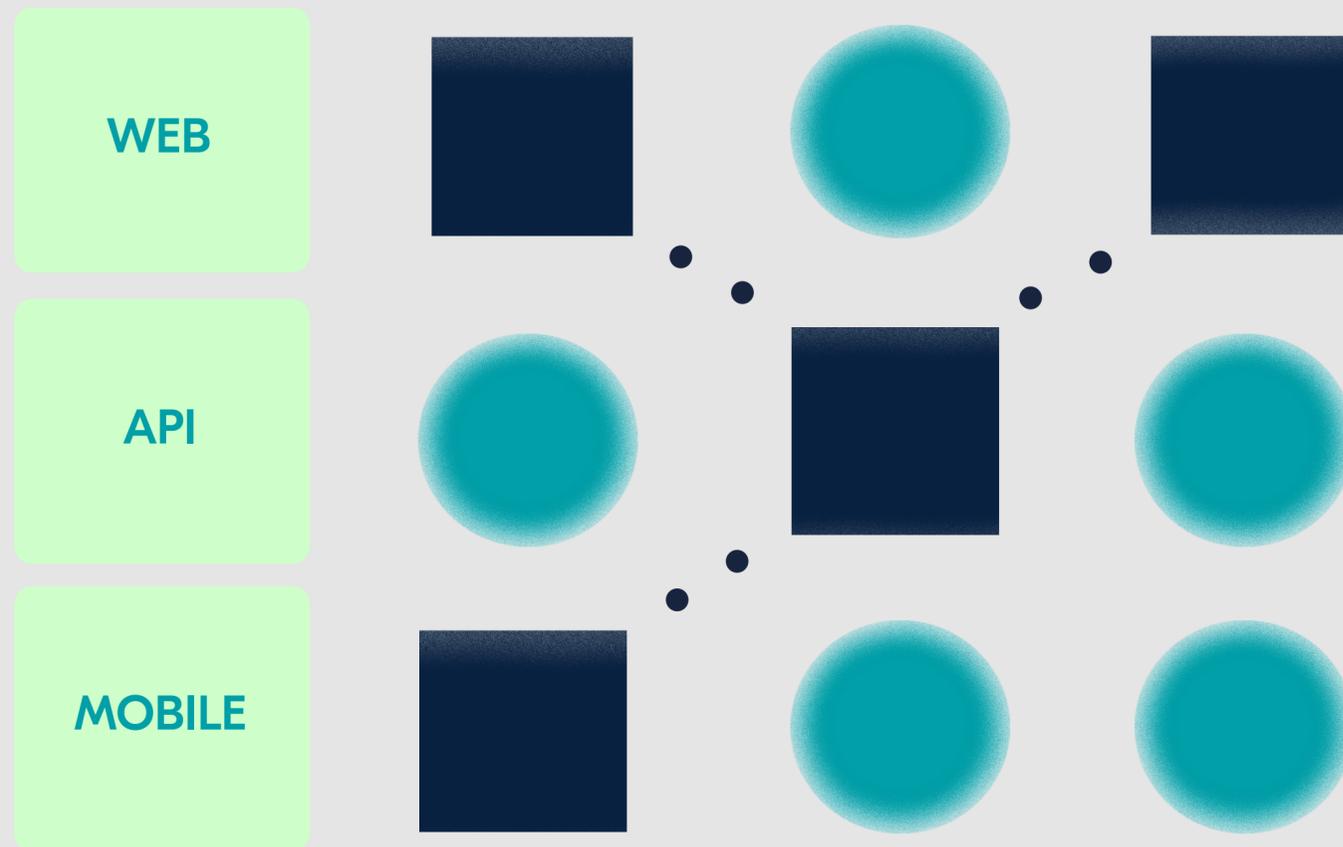
Device ID.



Threat intelligence.



Behavioral biometrics.



1.3 Cross dimension and channel correlation

Cleafy can correlate Indicators of Compromise (IOC's) identified on different dimensions to detect attacks that would go undetected by just performing a session-level analysis and without multidimensional correlation.

This is possible thanks to Cleafy's risk engine that evaluates the risk of each recorded event in real-time and propagates it at the session level.

In a world where activities are more and more completed across digital channels, connecting the dots beyond the traditional single dimension analysis is essential.

It's like having million eyes.

2. Stay one step ahead

After many years of experience in the banking and financial online fraud detection industry, Cleafy owns a **deep knowledge of a wide range of threats** and can develop an **optimal prevention and protection strategy** tailored to your business needs.

Our **Threat Intelligence team** includes skilled fraud hunters whose every day's goal is to uncover fraudsters, follow their trail and study their moves.

Once they catch a threat for the first time, they classify it in the platform and make it visible for you in real time. In this way, every time the classified pattern occurs, the platform will recognize it automatically.

For you, this means:

Complete visibility of every new malicious pattern hitting your users, including zero-day threats

Access to Early Warning Technical Reports with a detailed analysis of every new threat.

Stay updated on suspicious mule accounts and payee anomalies.

Benefit from concrete support if you are under attack and need help to make the right moves.

With all this information, you'll be able to set your optimal security posture, configure your automated responses, and minimize your risk exposure. All this, without leaving Cleafy dashboard.

Thanks to our tailored up-to-date Threat Intelligence data and insights, you'll stay ahead of fraudsters' moves.

3. Move fast and precisely

Once the threats are identified, Cleafy makes it possible to **move fast and precisely** by automating pattern-based response actions.

Today, the majority of fraud management solutions base their threat responses on **pre-defined risk thresholds**, meaning that the system assigns a risk score to each activity independently of the context in which the activity takes place.

By relying on this approach, it becomes easier to miss potential frauds or to create persistent frictions to the end-user.

Cleafy **sees everything** that happens in the user's journey and can respond dynamically to each micro-pattern identified. It's what we call a **granular response**.

What does this mean to you?

- Minimum risk
- Great application usability
- Timely fraud response

By deploying adaptive response mechanisms based on patterns, we'll help you deal with any scenario in the best possible way.

**Benefits
for you**

**Know your
users**

**Stay one
step ahead**

**Move fast
and precisely**

**Granular
end-to-end visibility**

**Multi-dimensional
analysis**

**Continuous event
correlation**



Actual real-time

**Tailored Threat
intelligence**

**Automated pattern-
based response**

**Benefits for
your customers**

**Complete
safety**

**Seamless
experience**

**Privacy
guaranteed**

SaaS deployment

In partnership with Google Cloud, Cleafy Platform is provided as SaaS. This gives immediate access to all threat detection capabilities without the need to invest in new hardware.

Real-time support and updates

The SaaS platform gets continuously updated by the Cleafy Threat Intelligence team with the latest data and insights. Easily readable tags will indicate when a complex threat gets recognized.

Easy integration with existing systems

All features are accessible online and easily integrable with your current systems, without the need to download further applications or adjust the other tools in place.

Complete data control and privacy policy compliance

All data is stored and completely accessible online. Data Centers are based in Europe, retained and processed in compliance with the GDPR privacy and security law.



Our customers'
voice



Cleafy's rating

5.0



based on reviews in the last 12 months

CISO
Top 10 italian banks

“Thanks to Cleafy we can detect targeted attacks, prevent frauds, and reduce false positives; the efficiency of our small fraud management team has largely improved.”

Head of Security
New-generation digital bank in EU

“We rely on Cleafy's technology and intelligence services to detect attacks to our digital channels and minimize the impact on our users.”

Service Manager
Top 3 Payment Service Providers in EU

“Thanks to Cleafy, we are now able to deliver the best-in-class fraud management service and ensure PSD2 compliance to our customers.”



.Cleafy

Success Story:
Digital banking made safe and seamless

Introduction

Cleafy had the opportunity to support a European digital bank in **improving its internal security** to maximize customer experience and reduce fraud. With more than 8 million digital clients between Retail and Corporate Banking, our client's priority was to maintain the **smoothest user fruition of financial services** while keeping the focus in innovating its offering.

The story

A key player in digital banking, the bank was **expanding its innovative digital services** through web and mobile channels to satisfy a rapidly growing demand. In order to satisfy its users' needs, our customer was looking to consistently increase its systems' protection from online attacks and threats.

The tools already deployed consisted of a transactional monitor, a biometric solution, a behavioral solution, an adaptive authentication module and a risk engine acting as an orchestrator with a very strict security policy.

The challenge

When exceeding a low-risk threshold, multiple factors were requested or the operation/client was blocked, sending each individual case to the operations team for analysis.

This generated a large number of false positives, an impact on operations (high number of case reviews and customer contacts) and on the call center (a large number of calls from customers affected by account blocking).

Losses were growing due to the increase in digital fraud attacks (phishing, vishing, smishing, malware) that could not be fully detected and/or responded to in time with the solutions in place.

The solution

Cleafy offered a proof of value (PoV) covering the website application.

After the solution was installed, it took only about 3 weeks to evaluate the first results on real traffic. This was possible because **Cleafy did not require complex integration** and could be managed by a group of three analysts.

Once the test was successfully completed, Cleafy's deployment was agreed upon and extended to customer applications and mobile. In less than 3 months from the start of the PoV to the end of the project, our team successfully completed the threat analysis and investigation activity.

The outcome

Cleafy managed to provide **complete visibility of the customers' digital journey** by monitoring all their transactions with the bank, providing intelligence through multiple analyses, real-time correlation of all activity across channels, as well as integration with third parties (adaptive authentication solution, alerting module, transaction blocking module).

Cleafy's ability to provide a single environment for threat analysis, rule creation and automatic action configuration helped the team to improve their work from analyzing false positives to creating advanced rules for detecting and responding to attacks.

Increased level of security

+94%
frauds detected

The bank saw a consistent increase of attacks detected during new tailored campaigns, and a 20% reduction in losses over existing campaigns (attacks already detected by previously implemented tools).

Better customer experience

+30%
usability of digital services

The block of transactions and clients, calls to the support center and the requests for 2FA in transactional operations were significantly reduced.

Higher operational efficiency

-90%
open cases

The bank's fraud management team decreased the number of monthly cases from 5000 to 450 thanks to the improvement in visibility and automated responses.

Overall, the deployment of Cleafy helped the bank to enhance the existing solutions' capabilities and to increase the Return On Investment already made.

.leafy

Your freedom to look ahead

Innovating means looking the future straight in the eye, having a vision, and making it real.

That's how we want technology to be: continuous progress for serving people's needs.

We know that looking ahead requires safety and the assurance that everything is under control.

That's why we are here.

To help you build a digital ecosystem where your business can flourish safely through continuous innovation.

So go on. Do what you haven't done yet, try what you haven't tried yet.

We've got your back.



Making technology a safer place

If you want to learn more about how we can help you,
visit cleafy.com or email us at info@cleafy.com

© 2021 Cleafy S.p.A.
