Customer success story

Leading European Bank reduces wasted fraud checks by 90%

Enhances detection and customer experience with a three-person team.

.Cleafy

At a glance

The bank

- **Pan-European** institution
- **Over 8 million** digital customers
- Multi-country presence across **retail and SME** segments

The challenge

- Rising wave of **digital fraud attacks**
- Friction for genuine customers caused by **false positives**
- Analysts swamped by **fragmented signals**
- Too many **tools**, not enough **clarity**

The Cleafy advantage

- Unified fraud and threat detection
- Visibility across web and mobile channels
- Real-time detection and response
- Works with existing systems

Impactful results

- Fraud losses down 20%
- False positives cut by 90%
- The entire fraud operations managed by a 3-person team

Growth opened doors. Criminals walked right in.

With digital adoption accelerating, threats soon followed.

When this European bank expanded its online and mobile services, millions of customers came on board. Along with them came a different kind of visitor: **organised fraud groups** using phishing, malware, remote access, and subtle manipulation to get past defences.

The bank's security stack looked strong: transaction monitoring, behavioural biometrics, adaptive authentication, and a risk engine tying it together. But the day-to-day reality told a different story.

Alerts flooded in, and false positives persisted at a high rate. Every flagged login or transfer meant extra checks, blocked transactions, or lengthy manual reviews. Genuine customers were caught in the net, yet the fraud still slipped through.

The fraud team spent more time **chasing scattered signals** than stopping crime. Criminals were adapting quickly, and pressure was coming from every direction.

What was missing wasn't more data, it was connection

The attacks weren't high in volume, but they were highly targeted. Social engineering. Remote access. Device manipulation. All looking "normal" to the bank's legacy tools.

Fraudsters could guide customers through transfers on the phone, inject malicious scripts, or alter session content, all without changing devices or triggering login risk flags. Transactions passed every check until the **money was already gone**.

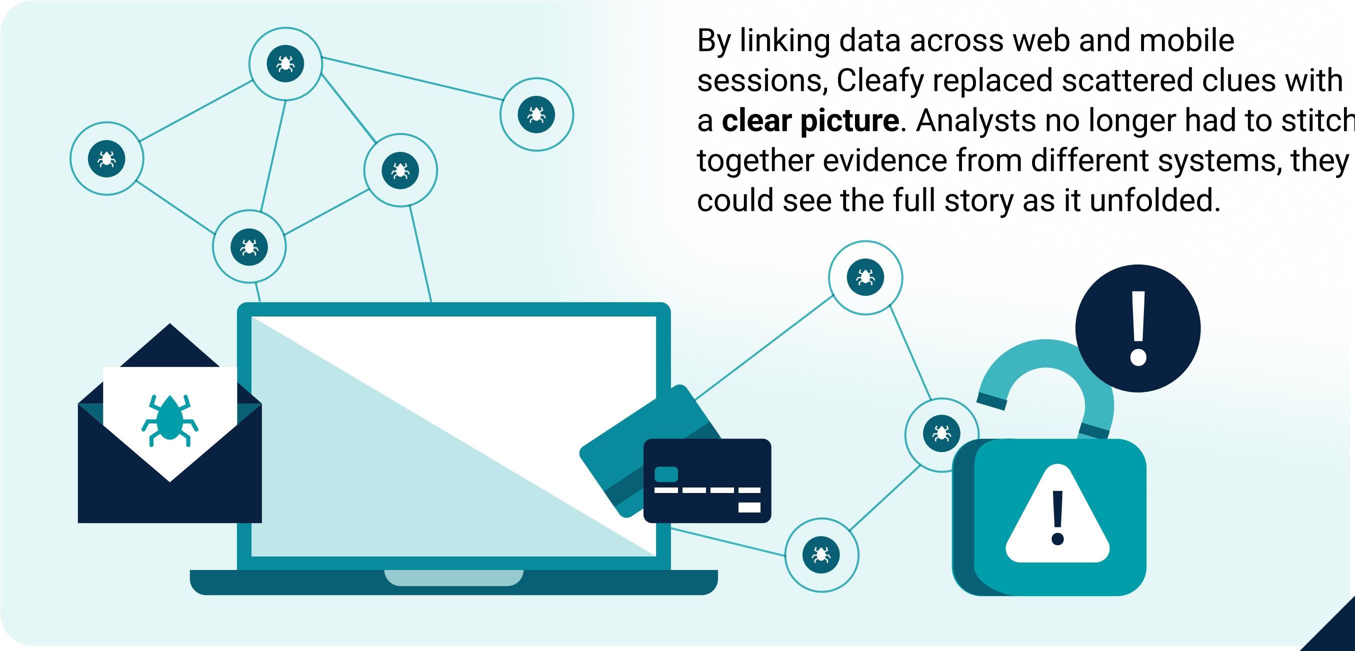
A clear view, at last

The bank rolled out Cleafy in three phases, starting with a live **proof of value**.

Within weeks, Cleafy was surfacing activity they'd never been able to see before:

- Injected fields in forms
- Remote control signals
- Scripted navigation patterns
- Tampered transaction flows
- Content mismatches pointing to manipulation

By linking data across web and mobile sessions, Cleafy replaced scattered clues with a **clear picture**. Analysts no longer had to stitch together evidence from different systems, they could see the full story as it unfolded.



What changed

> 20% fewer fraud losses

Attacks were intercepted before funds left accounts, including targeted campaigns that had previously gone undetected.

> 90% fewer false positives

Monthly case volumes fell from over 5,000 to a few hundred. The fraud team could finally focus on cases that mattered.

> Better customer experience

Friction dropped by 30%. Fewer unnecessary checks, fewer blocked transactions, fewer complaints.

> No extra headcount

A three-person team now runs the entire operation - detection through to decision - without firefighting or dashboard overload.

A different way of fighting fraud

This wasn't about adding yet another tool. It was about replacing fragmented views with **real visibility**, in real-time.

Now, the bank can spot and stop fraud **as it happens**, without slowing customers down or expanding the team.

Cleafy gave them the clarity to **stop chasing and start seeing**.

Learn more today

To learn more about how we can help you

> **Visit cleafy.com**

> **Email us at info@cleafy.com**

Trusted by leading European and LATAM banks, boasting a 4.2 score on Gartner Peer Reviews.

Gartner peerinsights™

Cleafy