Cleafy

NEXT-GENERATION ONLINE FRAUD DETECTION FOR NEW-GENERATION BANKS

CASE STUDY

A NEW-GENERATION BANK

Customers Bank is one of the fast-growing "new-generation" European banks. The Bank's mission was set to offer a wide range of financial products and services for individuals, families and businesses with a strong focus on delivering new levels of quality, service and efficiency, while also providing the best possible user experience "without losing the human connection," as articulated in their mission statement.

In the year since its foundation, the Bank has already been able to establish itself as a key player in a very competitive market by launching a brand-new online banking concept. In order to achieve this quite ambitious goal, the Bank made significant investments on both the most innovative banking platform and the most advanced information technology solutions.

Above all, the need for the Bank to deliver a new paradigm in user experience for online banking provided several challenges to their security team, as they were requested to minimize customer friction while supporting instant payment and open banking initiatives, and ensure regulatory compliance (PSD2). In particular, the anti-fraud team had to select and implement the best fraud detection solution to ensure the Bank would quickly gain an excellent reputation in the market by delivering the best customer satisfaction in terms of protection against online frauds.

> *"We are very satisfied with the choice we made for our Online Fraud Detection solution. Cleafy allowed us to stay focused on our ambitious development plan. Both the technology and the team exceeded our expectations, by quickly delivering value and adjusting to our needs."*
>
> *– Bank CISO, new-generation European Bank*

> *"Today's banking initiatives may expose to new fraud scenarios that need to be addressed effectively and immediately. That is why we needed a product with a high degree of confidence and a low false positive rate, while transparently integrating with our applications."*
>
> *– Bank CISO, new-generation European bank*

THE BANK REQUIREMENTS

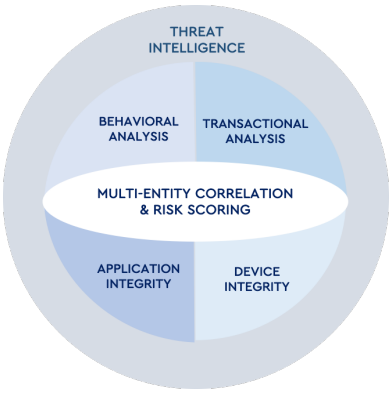
To select the fraud detection solution, the Bank defined several functional and non-functional requirements. The following three were the most critical, as aligned to their business goals:

- The first requirement was to **minimally impact the application lifecycle and technology stack** to guarantee the fastest time-to-market of new business functionalities. Of course, for a new-generation dynamic bank, this was a "no-go." As a matter of fact, many other solutions were immediately discarded because of this critical requirement.
- A second critical requirement was related to the ability to monitor all channels (web, mobile and API) and be able to **detect frauds in real time with low rates of false positives** and to **automatically trigger responses.** These features are critical to enabling smooth onboarding of new customers and to safely process instant payments where there is no time for any manual scrutiny.
- A no less important requirement was how easily the solution could be leveraged by the fraud analysts and the operational effort to maintain and manage the solution over time, as the anti-fraud team could count on very few resources. Indeed, the expectation by the Bank was that the chosen solution would enable the maximum level of automation to support a lean and agile organization.

CLEAFY DIFFERENTIATORS

Cleafy differentiators emerged during the POC (as described in further detail in the following).

- Cleafy's **application-transparent approach** does not require instrumenting or even touching applications. Cleafy passive and dynamic delivery of controls allows security to be decoupled from application development & deployment, and is a critical functionality that can be independently delivered and managed by the security team.
- While Cleafy was initially selected due to its **unique real-time detection** of endpoint side attacks, once in production, behavioral & transactional analyses were activated, and automated response rules were deployed.



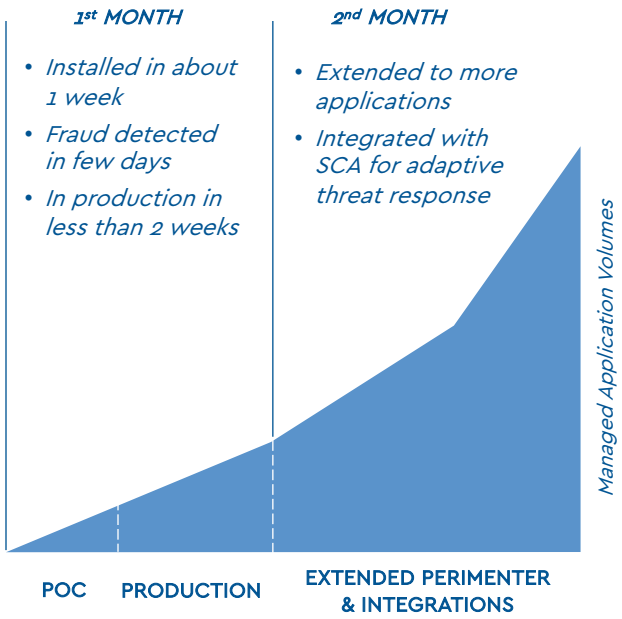
- Finally, when compared to other tools, Cleafy's **ease of setup, configuration and tuning** were striking. Cleafy was a perfect fit in terms of easily deploying new models and response mechanisms, configuring new applications and integrating within the Bank's ecosystem.

IN PRODUCTION IN JUST 2 WEEKS…

In less than one week, Cleafy was fully operational in a POC environment after smoothly integrating the application delivery infrastructure and without any change to the managed applications.

After just a few days of continuously monitoring a portion of the production traffic, Cleafy started to detect some relevant threats caused by malicious web injections on the client side and identified the associated fraudulent activities.

As a consequence, Cleafy's initial monitoring scope for the POC was immediately extended to the full production traffic (in less than 2 weeks), in the following months extended to other applications, and integrated to support risk-based, adaptive authentication.



… AND STILL CONTINUING TO DELIVER VALUE

Today, Cleafy continues to deliver value to the Bank analysts who are now able to:

- Investigate any suspicious activity in minutes, by leveraging Cleafy discovery capabilities and query language to explore relationship among users, endpoint, payee and bank account across multi sessions and channels.
- Take advantage of Cleafy Threat Intelligence feeds and the ability to leverage 3rd-party feeds related to blacklisted IPs and mule Bank Accounts such as those provided by industry consortiums.
- Quickly put in place modeling rules to automatically characterize suspicious patterns and trigger automated actions.

Thanks to Cleafy, the Banks has been able to anticipate several Account Takeover (ATO) and Automatic Transfer System (ATS) campaigns.

> *"Cleafy provides non-invasive application monitoring, comprehensive threat detection capabilities and flexible fraud scenario modeling that are essential to protecting modern payment systems."*
>
> *– Bank CISO, new-generation European Bank*

TANGIBLE BUSINESS BENEFITS

Thanks to Cleafy, the Bank is now able to:

- **Launch new marketing initiatives** without compromising on security and while staying compliant with regulations (PSD2)
- **Deliver a no-friction user experience** along the entire digital journey, starting from the onboarding phase
- **Avoid money losses and reputational issues** by keeping users protected against today's sophisticated online frauds
- **Improve operational efficiency** thanks to shortened time to investigate cases and automated real-time responses
- **Adapt the security posture** in response to an ever-evolving cyber fraud landscape by detecting attacks in the early stages
- **Make security a business enabler,** not a required priority or unavoidable cost by improving the overall user satisfaction

OUR PROMISE

Whether you are running a new-generation bank or delivering any other critical online service, you need next-generation online fraud detection to keep your users and business protected

Assessing the value of Cleafy only takes few days – we promise Cleafy will exceed your expectations!

CLEAFY

Cleafy solutions are based on patented threat detection & protection technology successfully adopted by leading banks and financial services and today protecting millions of online users.

Contact us at info@cleafy.com

MILAN • FRANKFURT • LUBJIANA • MADRID • PRAHA • SEVILLA • BOSTON