Use Case

Accurately detect and prevent Automated Transfer System (ATS) fraud

Automated Transfer System (ATS) attacks exploit gaps between user interactions and security protocols, manipulating legitimate transactions without user awareness.

These sophisticated attacks mimic genuine user behaviour, **bypassing traditional behavioural detection systems**. Delivered through malware, often via phishing or smishing, ATS attacks are both **automated and scalable**, making them challenging to trace and combat. Their ability to evade conventional fraud detection methods and affect numerous accounts without direct access to victim accounts presents a significant challenge.

The need for advanced malware detection

PSD2 regulations demand financial institutions implement advanced malware detection. Simple detection of fraud outcomes isn't enough, as the initial fraud might be invisible until it's too late. Modern malware, powered by AI, can change its form to avoid detection, making it crucial **to identify even the smallest tampering** in application content. Effective fraud prevention combines data from various sources, such as malware indicators, destination account flags, historical patterns, and tailored threat intelligence.

Real-time protection for every digital interaction

Cleafy excels where traditional fraud detection fails by detecting and characterising ATS attacks with **pinpoint precision**. It provides visibility into compromised endpoints and reveals the tactics used by attackers. Cleafy's **real-time protection** adjusts to sophisticated threats and reveals underlying infrastructure.

Cleafy's distinctive approach

1. **Granular visibility**
   Monitor every session for behavioural anomalies and malware presence, crucial for detecting ATS attacks early.

2. **Automated response at scale**
   Implement adaptive responses that scale with identified threats, securing your systems effectively.

3. **Real-time threat detection**
   Stop potential fraud in its tracks by detecting and neutralising threats immediately.

4. **Comprehensive risk control**
   Balance fraud prevention with a seamless user experience.

5. **Governance and compliance, simplified:** Cleafy's whitebox approach provides clear reasoning behind each classification, simplifying governance and compliance.

Cleafy's FxDR capabilities

Cleafy's FxDR platform offers real-time defence against advanced threats, including ATS attacks. Using patented technology, **Cleafy monitors and verifies application integrity on endpoints**, spotting malicious code and anomalies early. This approach allows Cleafy to prevent fraud before it escalates, **integrating advanced cybersecurity with fraud management** for full visibility across web and mobile channels. Cleafy's platform **provides accurate protection against ATS, ATO, APP fraud** (scams), and adapts to changing fraud tactics while minimising disruption.

Malware detection

Cleafy's patented technology ensures full content integrity, detecting subtle tampering and zero-day malware like SharkBot.

Real-time risk correlation

By correlating risk indicators with malware presence, Cleafy accurately identifies and addresses ATS attacks.

Tailored threat intelligence

Cleafy's platform is continuously updated with insights from our Threat Intelligence Team, automatically recognising and labelling advanced threats and ATS tactics.

Adaptive response

Cleafy integrates with existing systems to automate responses tailored to specific threats, improving threat management efficiency.

How it works

Identifying suspicious sessions

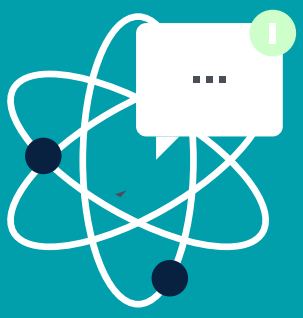
Advanced intelligence detects anomalies and flags threats, with key indicators presented in the Cleafy dashboard for quick assessment.

Classifying threats and connecting the dots

Once a suspicious session is flagged, Cleafy's granular visibility allows detailed analysis of risk indicators, helping analysts connect data across sessions for informed decision-making.

Automating detection and responding at scale

Cleafy's smart logic automates responses based on threat patterns, ensuring real-time, scalable protection across all scenarios



Cleafy customers experience

97% reduction in unnecessary Strong Customer Authentication (SCA) requests and blocked transactions, enhancing the customer experience.

89% decrease in unresolved or active fraud cases, easing analysts' workload and boosting operational efficiency.

91% drop in attacks, resulting in significant financial savings.

Protecting against tomorrow's threats today

Global presence

Cleafy secures billions of transactions from over **100 million accounts globally.**

Innovation

79 technology patents and ongoing advancements.

Customer trust

100% customer retention year on year.

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 4.9 score on Gartner Peer Reviews.

Gartner peerinsights. 4.9