.Cleafy

Use Case

Proactive defence against Account Takeover (ATO) fraud

Account fraud, including **Account Takeovers** (ATOs) and **fake account creation**, poses a significant threat to financial institutions (FIs). Cybercriminals increasingly employ sophisticated methods—ranging from social engineering to advanced malware—to exploit security weaknesses for financial gain. Such attacks can lead to:

> **Compromised personal data:** Customer loss and privacy breaches.

> **Financial damage:** Unauthorised transactions and chargebacks.

> **Brand reputation harm:** Erosion of customer trust and user experience.

> **Regulatory penalties:** Increased notification costs and compliance risks.

Fraudsters often start by stealing personal credentials or login information. They use **social engineering tactics** like phishing and smishing or deploy **malware** on victims' devices. Advanced attacks typically combine these methods, employing both social engineering and malware to achieve their goals.

How Cleafy's FxDR protects against ATO fraud

Cleafy's Fraud Extended Detection and Response (FxDR) platform **integrates seamlessly with existing systems**, offering real-time protection. By monitoring user behaviour and business data signals from the start, Cleafy helps prevent ATOs and other forms of fraud from the outset.

Cleafy's distinctive approach

1

Granular visibility
Gain comprehensive insights into each session, including geo-location, behavioural anomalies, and malware presence—critical for early threat detection.

2

Accurately anticipate and counter threat attacks before fraud occurs
Recognise attack patterns early, reducing false positives and protecting legitimate users.

3

Automated response at scale
Deploy automated responses that adapt to identified threats, ensuring robust and scalable protection across your systems.

4

Real-time threat detection
Detect and neutralise threats in real-time, preventing potential fraud before it impacts your organisation.

5

Comprehensive risk control
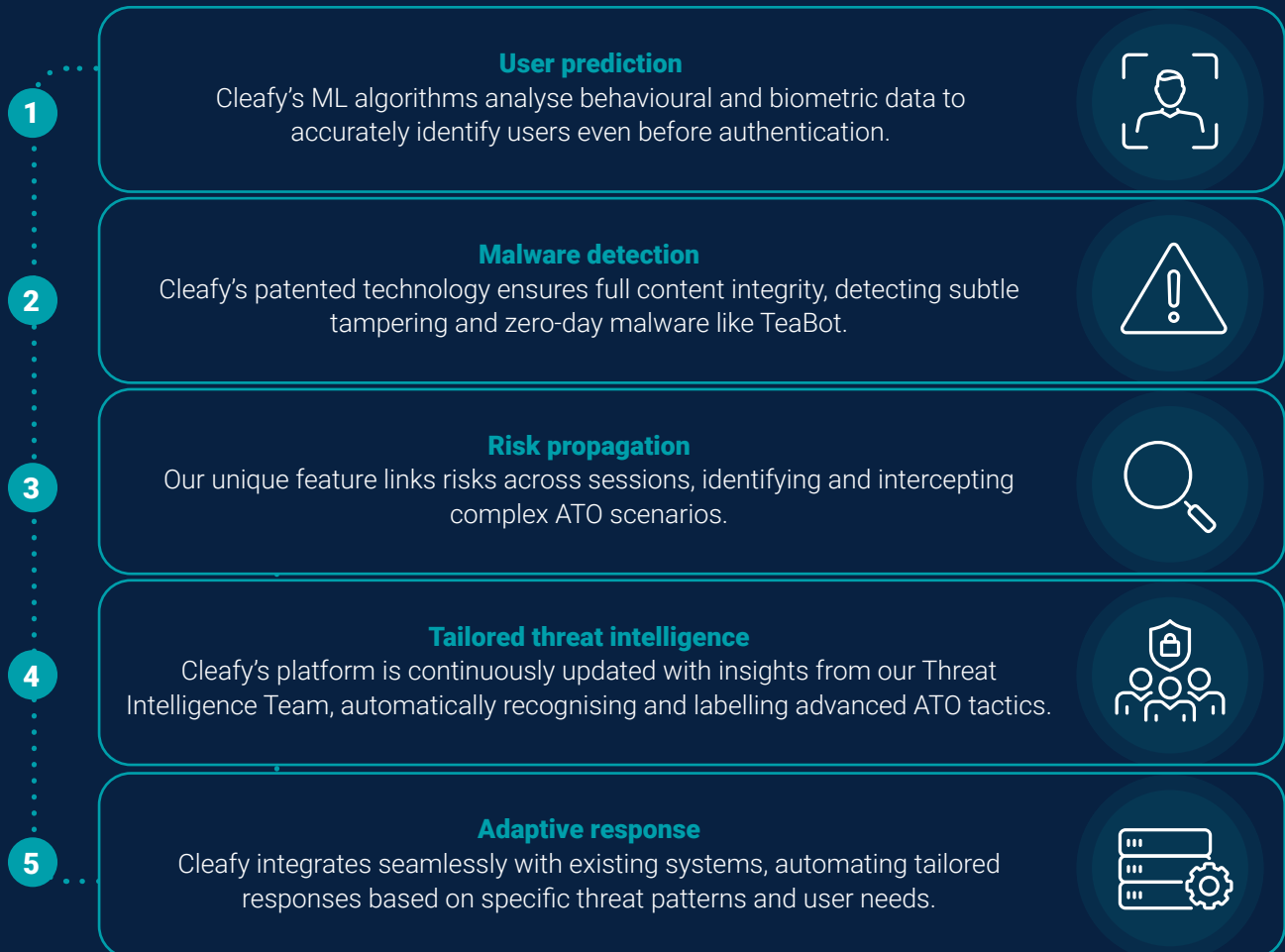Minimise the impact of fraud while maintaining a seamless and frictionless user experience.

6

Target fraud at its source:
Cleafy's zero trust model ensures continuous verification of access attempts, reducing the risk of unauthorised account access.

Cleafy's FxDR capabilities

Cleafy identifies and neutralises threats in real-time, stopping attacks before they turn into fraud. It empowers financial institutions to adopt a proactive approach to counter today's and future threats. As an **FxDR platform, Cleafy combines advanced cybersecurity with fraud management in a unified system.** This integration provides full visibility across web and mobile channels throughout the entire customer journey, from pre-login to transaction completion. Our FxDR platform provides **precise protection against ATO, ATS fraud, APP scams,** and more, adapting to the evolving tactics used by fraudsters while minimising disruption.

1

User prediction
Cleafy's ML algorithms analyse behavioural and biometric data to accurately identify users even before authentication.

2

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

3

Risk propagation
Our unique feature links risks across sessions, identifying and intercepting complex ATO scenarios.

4

Tailored threat intelligence
Cleafy's platform is continuously updated with insights from our Threat Intelligence Team, automatically recognising and labelling advanced ATO tactics.

5

Adaptive response
Cleafy integrates seamlessly with existing systems, automating tailored responses based on specific threat patterns and user needs.

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
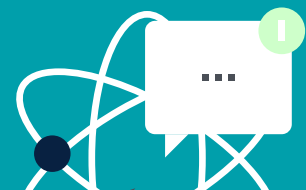
Cleafy customers experience

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 ★★★★★ 4.9
peerinsights.

.Cleafy