.Cleafy

2021

Solution Brief

cleafy.com

Table of contents

Introduction

Fraud attacks across digital channels have increased notably in recent times, accelerating even more due to the recent push towards the digitalization of services observed during the Covid19 pandemic. raud prevention teams are rethinking the strategy to mitigate the risk without compromising the agility and growth of their businesses.

The **techniques used by fraudsters are more and more advanced,** making **it extremely challenging to detect attacks by following the traditional approach** adopted by anti-fraud departments: multiple teams working in silos and adopting multiple separated solutions.

The **new paradigm of full detection and response** is based on breaking these silos, having in the same tool multiple detection capabilities and the possibility to set-up automatic responses, that decrease the time to respond from days/weeks to seconds/minutes.

Cleafy is an innovative solution based on **patented technology**, specifically designed to protect online banking and financial services against advanced fraud on digital channels, such as those committed by means of Social Engineering identity theft (phishing, vishing, smishing), Malware attacks (Man-in-the -Browser, Man-in-the-Middle, RAT-in-the-Browser, APP repackaging, SMS theft, Mobile Overlay applications) and other attack vectors leveraged by fraudsters.

Cleafy ensures continuous **End-to-End visibility of the customer journey** across all digital channels. The platform applies multiple fraud detection analyses (customer behavior, device, transaction, etc.) to enable early identification of threats, and allows to set-up automated responses to stop those threats at scale.

The responses are configured via the platform itself as a series of actions that are executed when the risk level exceeds an assigned threshold (ex. raising the security level, requesting double factors, alerting the Anti-fraud teams, etc.).

Cleafy works **without the need to modify the service application and is completely transparent for the end user** (it doesn't require any type of agent installed on the users' device).

Cleafy provides threat protection capabilities and **can be integrated within any technology framework**, such as risk-based authentication systems, security information and event management systems (SIEM), transaction monitoring systems, hubs, etc.

Cleafy's customers see clear advantages for both their end users experience (reducing friction), and for their fraud prevention teams (reduction of false positives, deterministic identification of threats, detection of zero-day malware or in early stages, full visibility and automatic responses).

Why Cleafy

The adoption of digital payments market is expected to reach $175.8 billion by 2026, rising at a market grow of 20% CAGR over the forecast period, and it is also facilitated by the adoption of mobile devices across new segments of the global population [1].

The volume of attacks to online services provided by financial institutions is also growing fast (3.6x year over year) [2], for an estimated 1M users attacked across the globe in 2021, only considering banking trojans. Instant payments are expected to further exacerbate the issue.

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

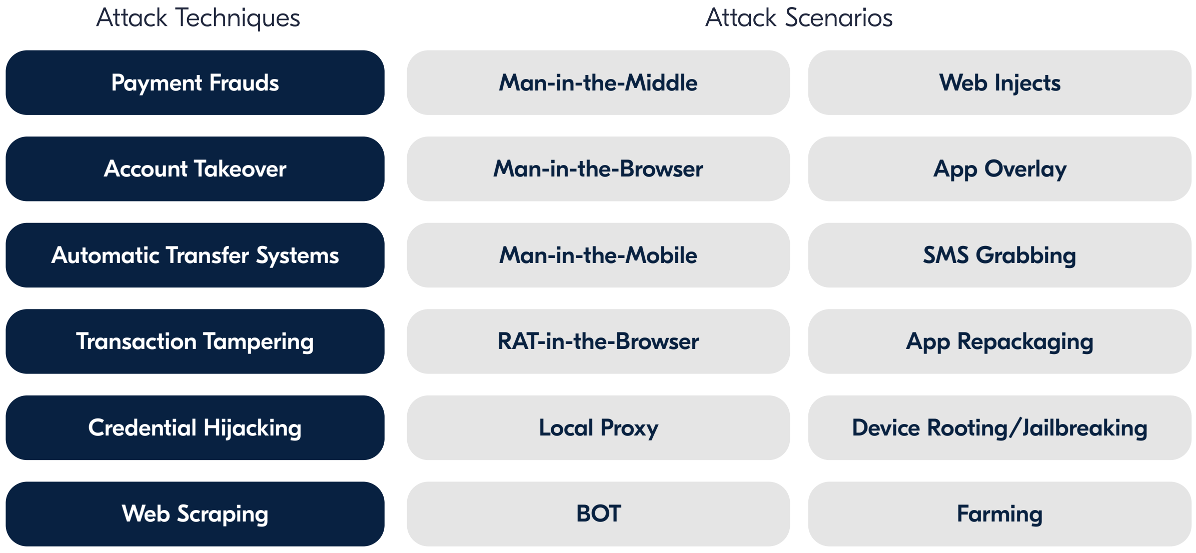
Traditional malware detection solutions based on signature and pattern matching are failing in detecting these advanced targeted attacks, as also testified by the yearly increase in the number of new malware variants for both web (+36%) and mobile (+54%) [2] [3].

The end-user devices, the endpoints, represent today the weakest link in the security chain when protecting online services; a new approach is required in order to prevent financial losses and reputational damages while avoiding introducing any friction for the user experience.

Moreover, the **PSD2 compliance requirements**, created with the aim of minimizing the risks of mistaken or fraudulent transactions, specifically include the ability to identify signs of malware infection on endpoints when assessing the risk of a transaction.

Cleafy is able to detect and analyze advance attacks based on **Man-in-the-Browser (MITB), Man-in-the-Middle (MITM), RAT-in-the-Browser, App Repackaging, SMS Grabbing, Mobile Overlay** and many other different attack vectors used by fraudsters to steal credentials or manipulate transactions.

Cleafy is also able to detect generic malware (code injection at the financial application level), phishing/pharming scenarios (cloning of the corporate site), **Web Scraping** (bots automatically downloading content from the corporate site). In the next figure we can see some of the attack scenarios and attack techniques recognized by Cleafy



Attack Techniques	Attack Scenarios	
Payment Frauds	Man-in-the-Middle	Web Injects
Account Takeover	Man-in-the-Browser	App Overlay
Automatic Transfer Systems	Man-in-the-Mobile	SMS Grabbing
Transaction Tampering	RAT-in-the-Browser	App Repackaging
Credential Hijacking	Local Proxy	Device Rooting/Jailbreaking
Web Scraping	BOT	Farming

Figure 1. Attack techniques and Scenarios

How it works

Cleafy's approach to on-line fraud detection is based on the **continuous monitoring of the application traffic** (even before the authentication phase) and **real-time assessment of the risk**. Based on the real-time risk scoring, Cleafy can automatically activate **adaptive threat responses**, including Cleafy dynamic application protection, according to the defined security posture.

Multiple Analyses

Cleafy analyzes the traffic generated between the end user and the application's server across all digital channel digital channels (Web, Mobile, API), even before the 'login', from the arrival to the main web page or the opening of the mobile application, until the end of the session. Information on behavior of the end user, device used (PC, mobile), content displayed, session, and traffic exchanged are sent in real-time to the Cleafy platform for analysis.

Cleafy divides its functionality into 4 pillars that act in real time:

- **End-to-end visibility** of the customer journey across all digital channels
- **Multi-dimensional Analysis** (including user behavior, transactions, malware and device integrity)
- **Correlation** of events, sessions and analysis of all digital channels
- **Seamless integration** with third-party solutions (sending alerts by email, sending information through REST API, etc.).

Cleafy offers an fully comprehensive fraud detection and response platform.

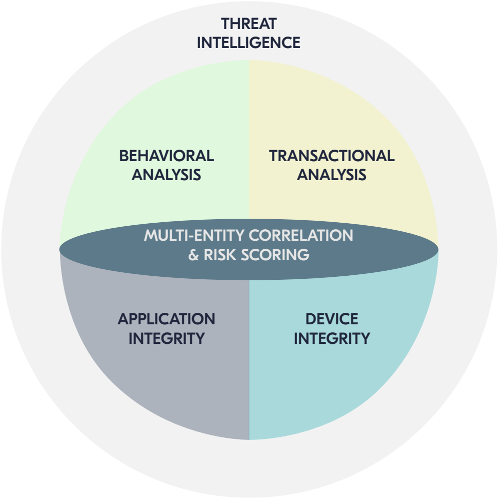


Figure 2. Cleafy multiple anlyses

End-to-end Visibility

The following figure illustrates how Cleafy can monitor the entire customer journey, even before the authentication phase, and continuously assesses the risk associated with the user session.

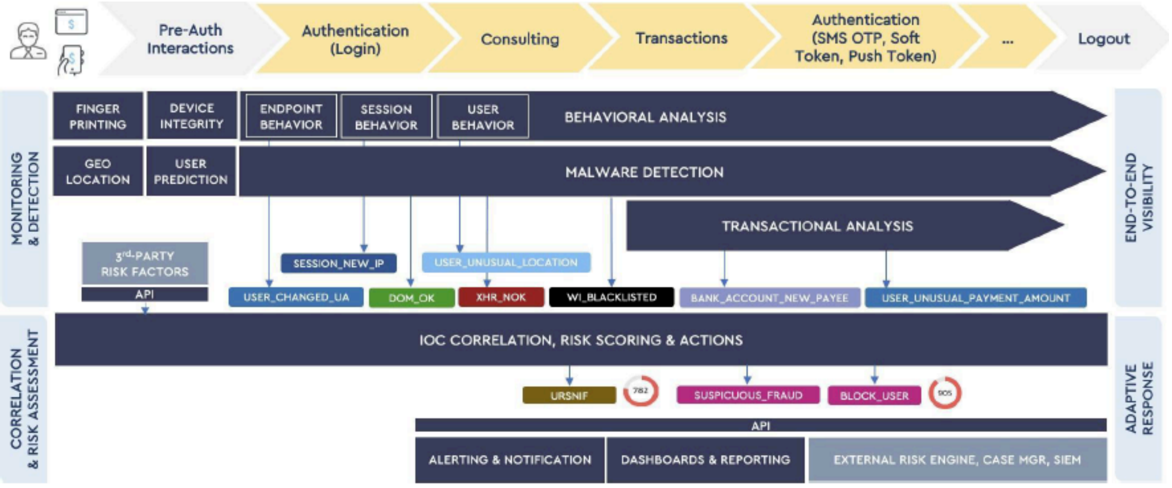


Figure 3. Cleafy monitors the entire customer journey

A key concept in Cleafy is the notion of **application integrity.** This notion emerges from the real-world experience that once an endpoint has been infected by banking trojan malware, malicious code will be injected into the delivered application content in order to hijack credentials, tamper transactions and perform payment frauds: this means that the integrity of the application is compromised on the endpoint.

Today targeted attacks are designed to escape detection from signature based traditional anti-malware solutions, thus, often, attack campaigns are in full swing before they get identified and signatures and rules can be applied. Security and antifraud teams are either being overloaded by too many false positives or no high-risk alert is being raised in presence of massive campaigns and they have no clue on how attacks are being performed.

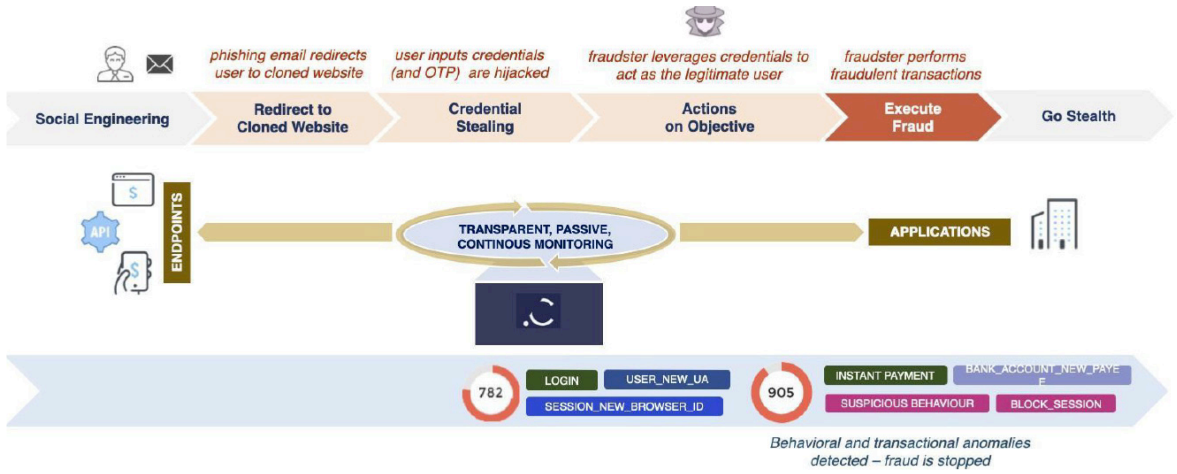

phishing email redirects user to cloned website
user inputs credentials (and OTP) are hijacked
fraudster leverages credentials to act as the legitimate user
fraudster performs fraudulent transactions
Social Engineering
Redirect to Cloned Website
Credential Stealing
Actions on Objective
Execute Fraud
Go Stealth
API
ENDPOINTS
TRANSPARENT, PASSIVE, CONTINOUS MONITORING
APPLICATIONS
782
LOGIN
USER_NEW_UA
SESSION_NEW_BROWSER_ID
905
INSTANT PAYMENT
BANK_ACCOUNT_NEW_PAYE E
SUSPICIOUS BEHAVIOUR
BLOCK_SESSION
Behavioral and transactional anomalies detected – fraud is stopped

Figure 4: Example of Cleafy detection of Account Take Over (ATO) attacks via phishing/farming

Cleafy patented application integrity detects in real-time any application tampering, **including from unknown and zero-day malware**, without generating false positives. When combined with device/browser fingerprinting, behavioral analysis and risk propagation, even complex attack scenarios involving parallel sessions issued by the fraudster, leveraging the user endpoint (by back-connecting via RAT tools), are identified by Cleafy as “high risk” and effectively countered via automatic threat response actions and Cleafy dynamic application protection.

Detection

Cleafy uses various techniques to detect advanced threats in real time, to discover infected or compromised devices, at every step of the user session, even before the authentication phase occurs. Cleafy detect complex attacks involving parallel sessions and client device use in real time (like using RAT tools). This is possible, thanks to the unique capabilities of the solution, such as: application, communication and device integrity; device/browser fingerprint, user behavior, risk propagation, with a flexible set of Indicators Of Compromise (IOC).

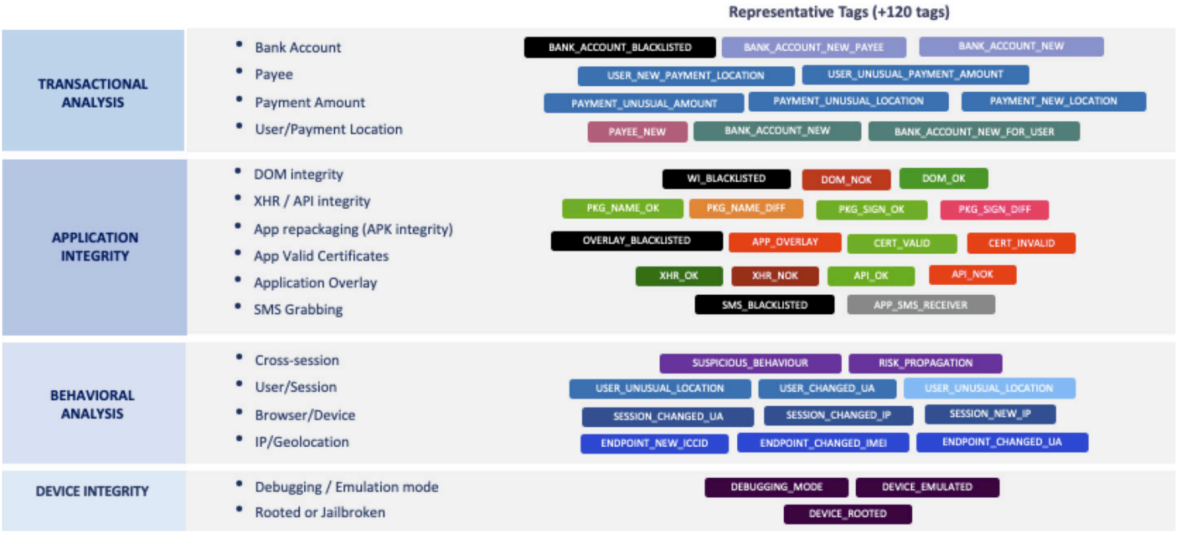


Figure 5. Predefined TAGs

Cleafy patented a detection technology for web applications that **verifies in real time the integrity of the application** sent to browsers (ex. injection of malicious code within the DOM, manipulations of the XHR/API). It detects deterministically any manipulation of the application, even those caused by zero-day Malware, without leading to any false positives.

Cleafy extracts fragments from the malicious code, giving the visibility required to exactly understand the techniques used by fraudsters; this information can be used to trigger different responses and improve the security posture, especially when correlated to the analysis of the behavior of the client under attack.

The evidence collected by Cleafy can then also help forensic investigations and analyses. Finally, the malicious code fragments are automatically grouped to be able to detect them even if they are modified over time, offering a predictive visibility of the evolution of the attack, better assessment of the associated risk and helping prioritize activities.

For mobile applications, Cleafy applies **detection techniques that verify device integrity** (ex. rooted or jailbroken devices), communications (ex. API call manipulation), and application level (application repackaging). For mobile device applications, the identified threats are represented by malicious or suspicious applications that are installed on the user's device and are used to steal credentials and one-time passwords (**OTP sniffing**) using window overlays (**overlay attacks**).

Correlation

Cleafy is based on the **continuous monitoring of all events** that occur with the interaction between the client and the application (e.g., HTTP requests and responses, XHR and calls to APIs), and collection of records of the use, or misuse, of the device/services offered. These events and sessions are evaluated by Cleafy's risk engine, **assigning the risk of each recorded event in real time, and propagating it at the session level**.

These risks are presented as labels (**TAGs**) that can be predefined (Cleafy offers more than 80 TAGs) or personalized; These labels with their corresponding risk score can be created, for example, with references to specific points of the application (e.g., login page, where credentials can be stolen) or user/device profiles (e.g., Infected devices) or other attributes that require specific tagging.
The following is an example of correlation where different checks are combined in real-time to detect complex attacks such as **ATO via phishing/malware attacks**:

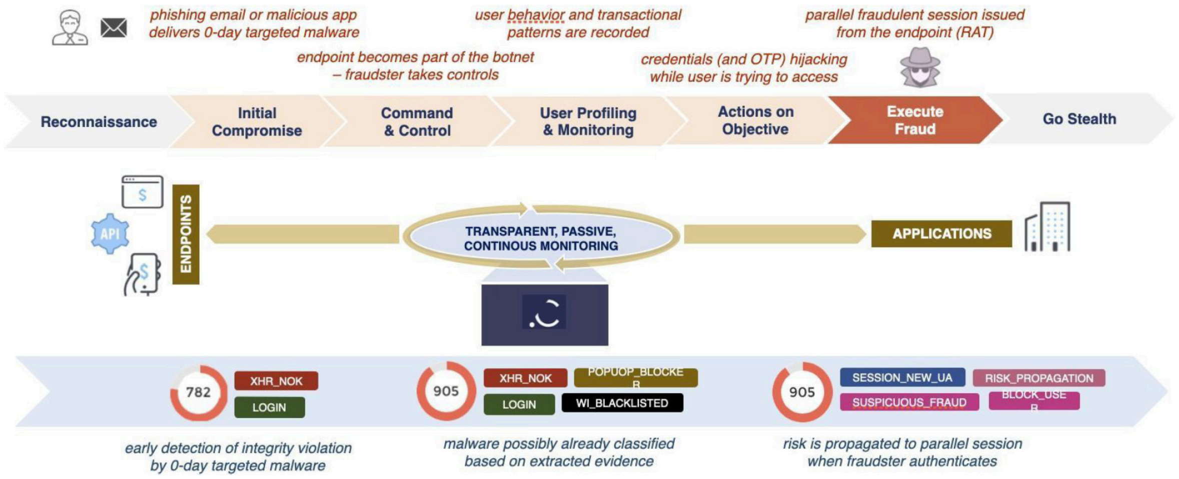

phishing email or malicious app delivers 0-day targeted malware
user behavior and transactional patterns are recorded
parallel fraudulent session issued from the endpoint (RAT)
endpoint becomes part of the botnet – fraudster takes controls
credentials (and OTP) hijacking while user is trying to access
Reconnaissance
Initial Compromise
Command & Control
User Profiling & Monitoring
Actions on Objective
Execute Fraud
Go Stealth
API
ENDPOINTS
TRANSPARENT, PASSIVE, CONTINOUS MONITORING
APPLICATIONS
782
XHR_NOK
LOGIN
905
XHR_NOK
POPUOP_BLOCKER
LOGIN
WI_BLACKLISTED
905
SESSION_NEW_UA
RISK_PROPAGATION
SUSPICUOUS_FRAUD
BLOCK_USER
early detection of integrity violation by 0-day targeted malware
malware possibly already classified based on extracted evidence
risk is propagated to parallel session when fraudster authenticates

Figure 6. Example of Cleafy detection of ATO via phishing/malware attack

Here another example of correlation where different checks are combined in real-time to detect SIM swap, another complex attack:

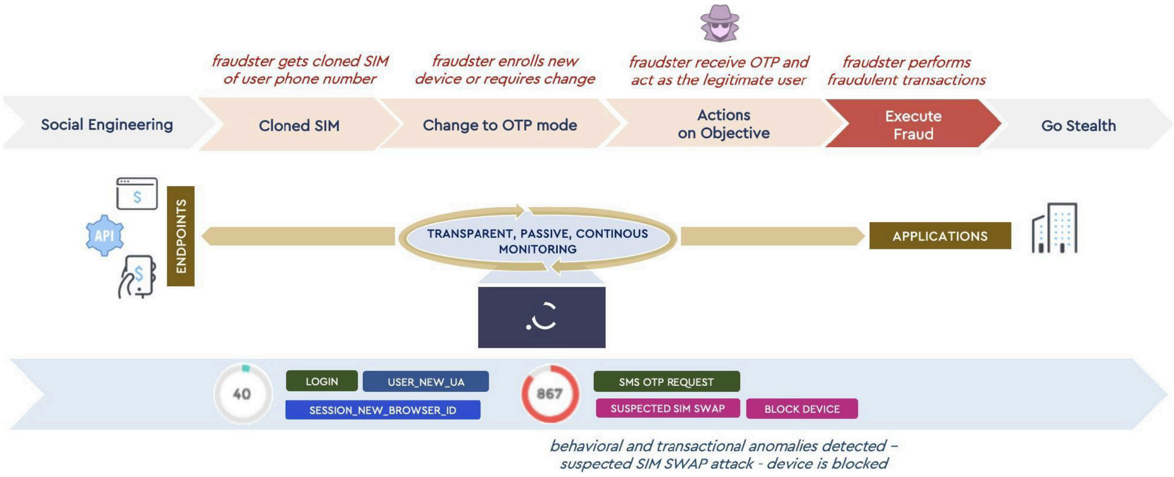

fraudster gets cloned SIM of user phone number
fraudster enrolls new device or requires change
fraudster receive OTP and act as the legitimate user
fraudster performs fraudulent transactions
Social Engineering
Cloned SIM
Change to OTP mode
Actions on Objective
Execute Fraud
Go Stealth
API
ENDPOINTS
TRANSPARENT, PASSIVE, CONTINOUS MONITORING
APPLICATIONS
40
LOGIN
USER_NEW_UA
SESSION_NEW_BROWSER_ID
867
SMS OTP REQUEST
SUSPECTED SIM SWAP
BLOCK DEVICE
behavioral and transactional anomalies detected – suspected SIM SWAP attack - device is blocked

Figure 7: Example of Cleafy detection of SIM Swap attacks

As Cleafy can manage multiple applications, it is possible to associate a different risk score for each managed application, establishing global risk scores that are inherited by all applications and, at the same time, allowing specific labels for each application to have a risk score different from the globally attributed value.

Automatic Actions

The Cleafy Rule Engine can automatically execute actions over complex threat scenarios, send alerts and notifications, execute threat responses, and invoke external modules (e.g. Adaptive Authentication module).

It is possible to define Rules with actions that are triggered when a specific threat is detected, and/or raise the risk level when a Malware infection, or compromised device, is detected.

The available actions are:

- **ADD TAG**: adding a specific TAG with a marked risk level for that event, session, application, threat, etc.
- **WEBHOOK**: sending any type of information to a REST API (risk score, session information, client information, etc.)
- **SEND EMAIL**: sending email with necessary information about the event, session, etc.
- **SLACK**: sending information through SLACK.
- **SYSLOG**: logging of the event and the necessary information in the syslog
- **CREATE THREAT**: opening a case on Cleafy dashboard with all the details needed to start the investigation

The integration of these capabilities in a unique platform offers anti-fraud teams the **ability to detect threats effectively and respond with precision and at scale**.
The final outcome is a dramatic reduction of fraud risk for instant services such as immediate transfers, digital onboarding, open-banking, etc.

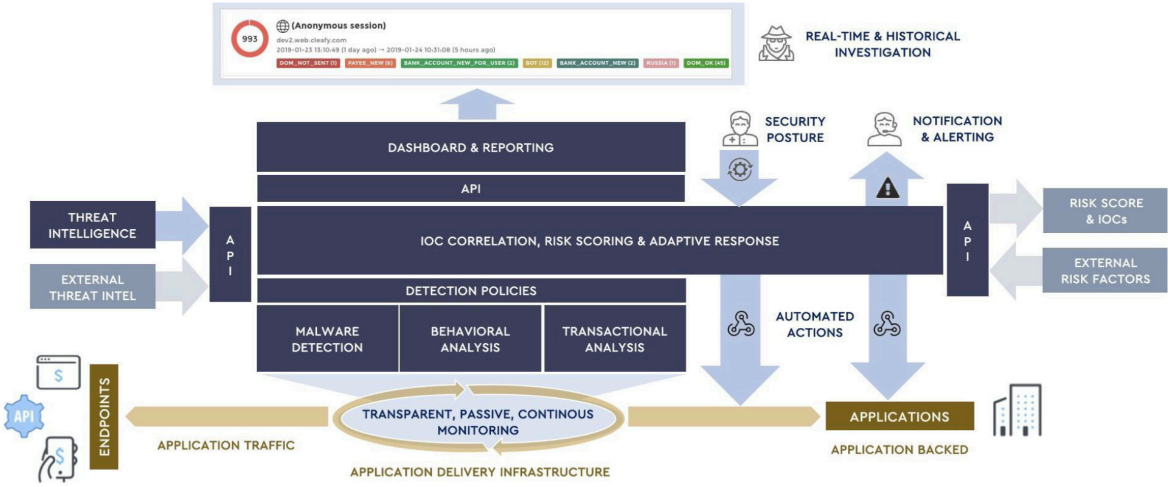


Figure 8. Overall logical Cleafy architecture with response actions triggered by detection

Cleafy Deployment

The deployment of Cleafy can follow two scenarios:

- the ADC/load balancer to inspect the traffic
- inject a Javascript, and the SDK in the mobile application.

It should be noted that Cleafy is completely "agent-less", not requiring the installation of any agent on the Web or on the mobile device. Cleafy is also fully transparent to the end user, does not affect the user experience and does not impact the performance of customer devices. Cleafy is also fully transparent to the web application, does not require any changes to the application and does not need to modify the components of the application's Backend.

To get the information, Cleafy makes use of an integration (with the ADC) and two components (Cleafy JS and Cleafy SDK) shown in the following high-level architecture:

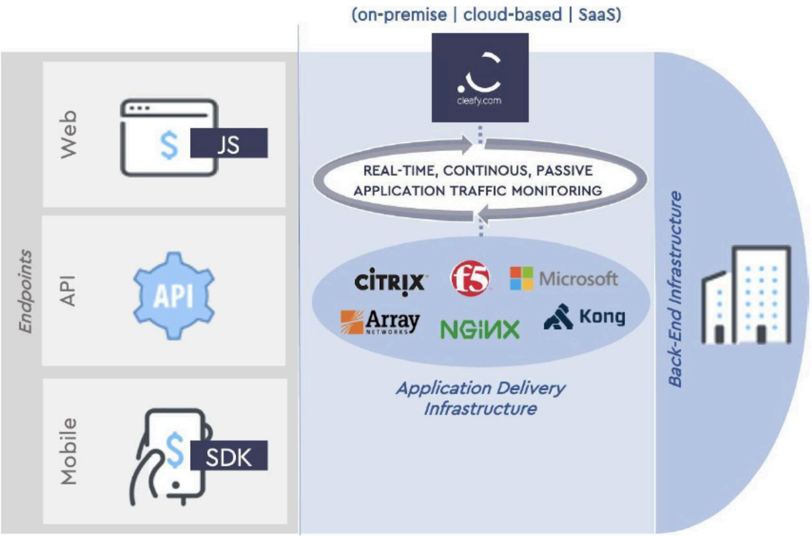

(on-premise | cloud-based | SaaS)
cleafy.com
Endpoints
Web
JS
API
API
Mobile
SDK
REAL-TIME, CONTINOUS, PASSIVE
APPLICATION TRAFFIC MONITORING
CITRIX
f5
Microsoft
Array NETWORKS
NGINX
Kong
Application Delivery Infrastructure
Back-End Infrastructure

Figure 9. High-level architecture

Deployment with the ADC

The Cleafy Platform integrates with the application delivery infrastructure, being this integration directly with the load balancer or with the ADC (Application Delivery Controller); In case neither of these components are available for integration, a reverse proxy called Cleafy Stream can be deployed. Hereafter, we refer to integration with the ADC as the Standard Integration Model.

Integration with the ADC provides Cleafy the ability to **inspect application traffic**. SSL/TLS traffic is required to be terminated at the ADC (or other integration point) level. The integration with the ADC also provides the **transparent injection mechanism of Cleafy JS** along with the application content that is sent to the client.

Cleafy has been integrated with most of the ADCs deployed in the market and specifically with Citrix NetScaler, Cleafy being a certified 'Citrix Ready Solution' (more information here).

The JavaScript automatically created by Cleafy is small and polymorphic, its typical size is less than 2KB (it depends on the detection options that have been enabled) and it does not impact the delivery of the application content to the client.

When delivered to the client's browser, Cleafy JS collects information from the environment and the content displayed by the browser (DOM) to be sent to the Cleafy Platform. All these communication is asynchronous and has no impact on the customer experience or device performance.

Deployment with the APP

Cleafy SDK is a small size library that is passively integrated into the mobile application, making the **customer experience and device performance unaffected**. Cleafy supports iOS and Android operating systems, as well as both native and hybrid applications (based on Cordova, or other development frameworks).

When the application is opened, a call to the library activates the module to send information to the Cleafy Platform, **without modifying the application logic**.

Cleafy in the financial ecosystem

Actual orchestrators or transaction monitors, that companies tended to use as the central point of integration, lack the detailed visibility of the user journey to respond dynamically to different threats. Relying their response in a static risk score, and not in the type of threat that needs to be countermeasure.

Cleafy introduced the detection and response model, not based on the usual risk score, but based on a granular response for different scenarios. Having full visibility of the type of threat, gives us the possibility to adjust the response, to better match the actual scenario.

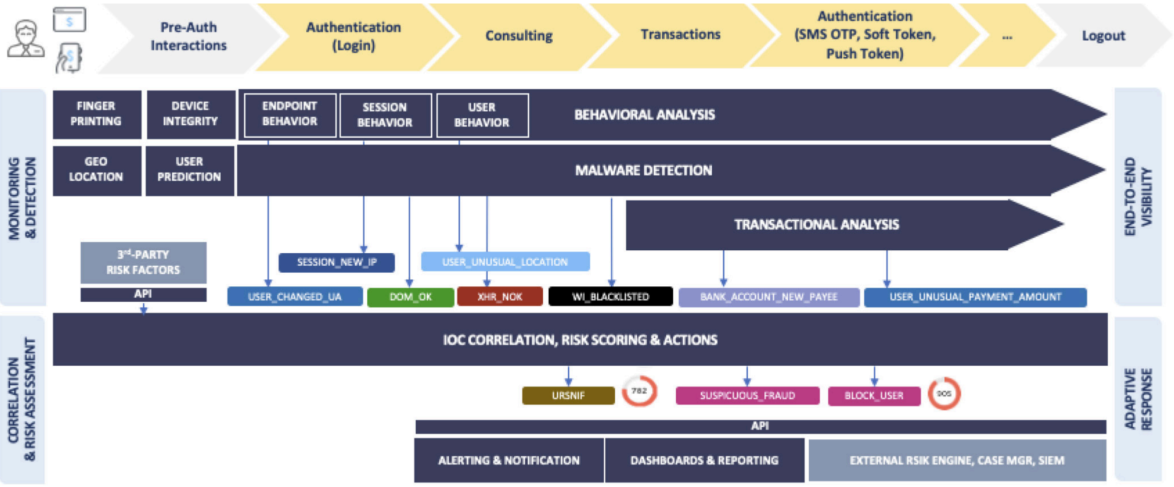
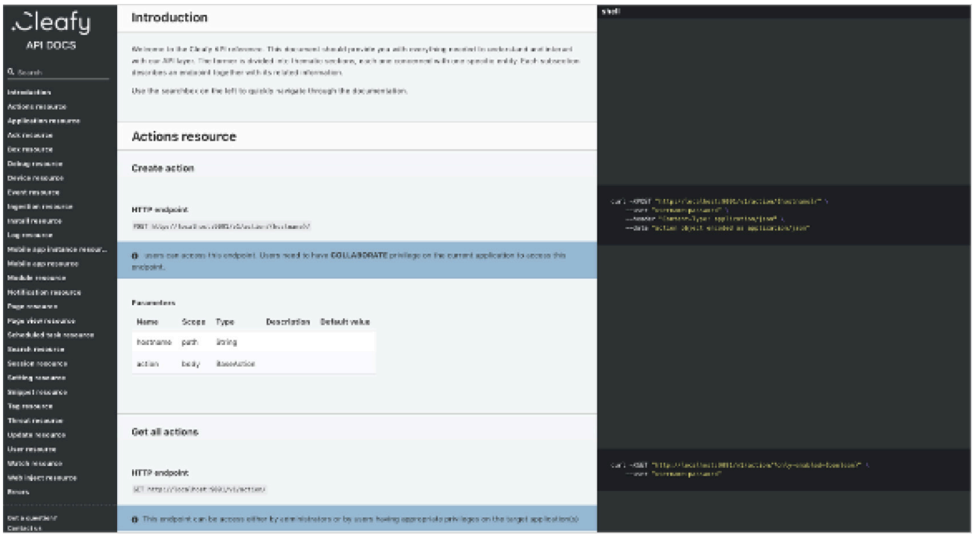


Figure 10. Adaptive response

Response mechanisms are based on a comprehensive set of customizable APIs (+200) and actions. These mechanisms can be leveraged to make **all the information collected from the devices in Cleafy** (e.g., context information about the device and monitored events) or generated by the Cleafy risk engine (including risk score, classification of threats and evidence), **available to any third-party solution**.



Introduction

Welcome to the Cleafy API reference. This document should provide you with everything needed to understand and interact with our API layer. The former is divided into thematic sections, each one concerned with one specific entity. Each subsection describes an endpoint together with its related information.

Use the searchbox on the left to quickly navigate through the documentation.

Actions resource

Create action

HTTP endpoint

[illegible]

users can access this endpoint. Users need to have COLLABORATE privilege on the current application to access this endpoint.

Parameters

Name	Scope	Type	Description	Default value
hostname	path	String		
action	body	BaseAction		

Get all actions

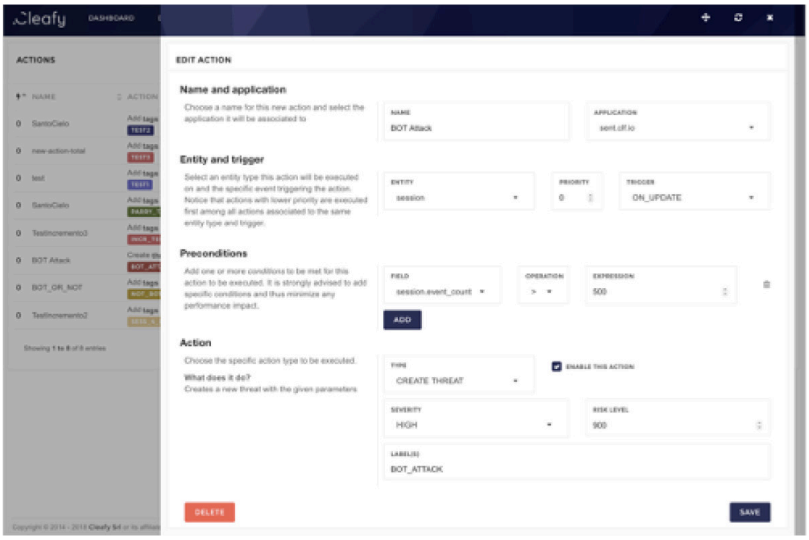
HTTP endpoint

[illegible]

This endpoint can be access either by administrators or by users having appropriate privileges on the target application(s)

Figure 11. APIs

Actions can also be used to integrate external systems, either by sending alerts and notifications (for example, via emails, syslog and Slack), or by invoking specific web links.



Cleafy
DASHBOARD
ACTIONS
NAME
ACTION
Showing 1 to 8 of 8 entries
Copyright © 2014 - 2018 Cleafy Srl or its affiliates
DELETE
SAVE
ADD

NAME	ACTION
0 SantoCielo	Add tags TEST2
0 new-action-total	Add tags TEST3
0 test	Add tags TEST1
0 SantoCielo	Add tags PARDY_T
0 TestIncremento3	Add tags INCR_TE
0 BOT Attack	Create thr BOT_ATT
0 BOT_OR_NOT	Add tags NOT_BO
0 TestIncremento2	Add tags SESS_A

EDIT ACTION

Name and application

Choose a name for this new action and select the application it will be associated to

NAME: BOT Attack

APPLICATION: sent.clf.io

Entity and trigger

Select an entity type this action will be executed on and the specific event triggering the action. Notice that actions with lower priority are executed first among all actions associated to the same entity type and trigger.

ENTITY: session

PRIORITY: 0

TRIGGER: ON_UPDATE

Preconditions

Add one or more conditions to be met for this action to be executed. It is strongly advised to add specific conditions and thus minimize any performance impact.

FIELD: session.event_count

OPERATION: >

EXPRESSION: 500

Action

Choose the specific action type to be executed.

What does it do?

Creates a new threat with the given parameters

TYPE: CREATE THREAT

☑ ENABLE THIS ACTION

SEVERITY: HIGH

RISK LEVEL: 900

LABEL(S): BOT_ATTACK

Figure 12. Actions

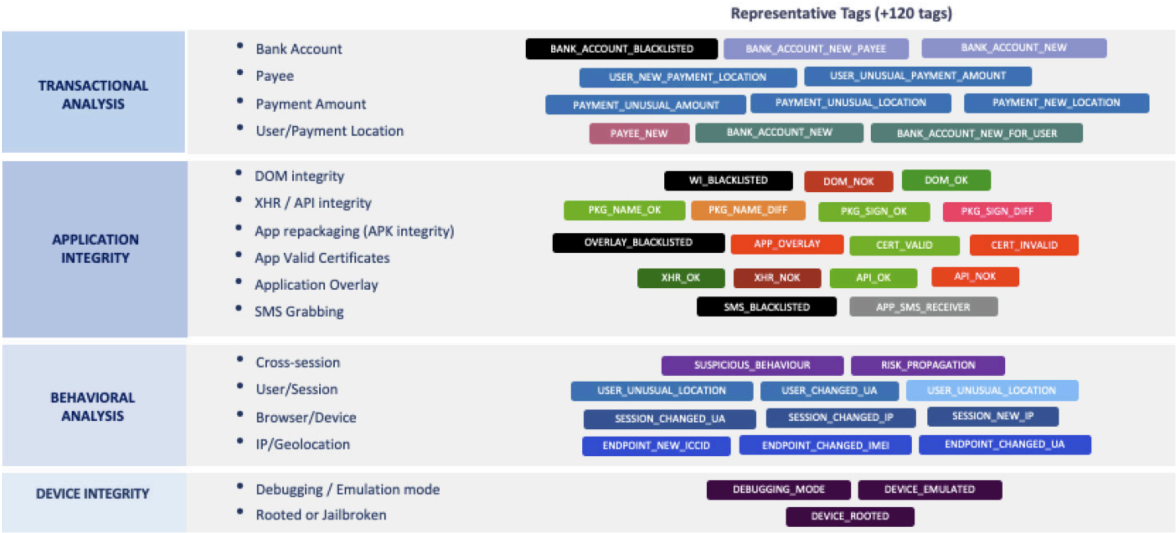
Cleafy is a complete platform for the detection of fraud attacks on digital channels, which **works without the need for the support of other tools or solutions**. But has also been designed to be easily integrated with components already deployed in the bank's ecosystem, supporting them and improving their analysis and reaction capacity.

Cleafy zero-day vision

CARTA approach

Cleafy was born years before the adoption of Continuous and Adaptive Risk and Trust Assessment approach (CARTA), but already completely in line with what Gartner recommend:

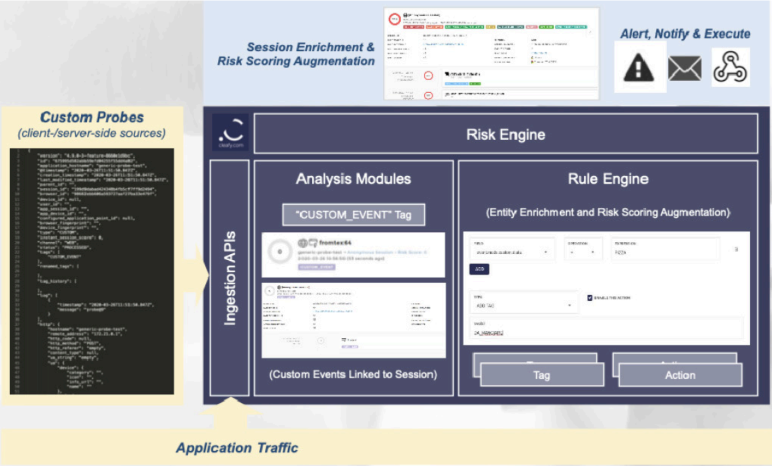
- Gather the broadest and deepest insights possible by deploying tools focused on malware detection, bot detection, behavioral analytics and device identification,among others.



		Representative Tags (+120 tags)
TRANSACTIONAL ANALYSIS	• Bank Account • Payee • Payment Amount • User/Payment Location	BANK_ACCOUNT_BLACKLISTED BANK_ACCOUNT_NEW_PAYEE BANK_ACCOUNT_NEW USER_NEW_PAYMENT_LOCATION USER_UNUSUAL_PAYMENT_AMOUNT PAYMENT_UNUSUAL_AMOUNT PAYMENT_UNUSUAL_LOCATION PAYMENT_NEW_LOCATION PAYEE_NEW BANK_ACCOUNT_NEW BANK_ACCOUNT_NEW_FOR_USER
APPLICATION INTEGRITY	• DOM integrity • XHR / API integrity • App repackaging (APK integrity) • App Valid Certificates • Application Overlay • SMS Grabbing	WI_BLACKLISTED DOM_NOK DOM_OK PKG_NAME_OK PKG_NAME_DIFF PKG_SIGN_OK PKG_SIGN_DIFF OVERLAY_BLACKLISTED APP_OVERLAY CERT_VALID CERT_INVALID XHR_OK XHR_NOK API_OK API_NOK SMS_BLACKLISTED APP_SMS_RECEIVER
BEHAVIORAL ANALYSIS	• Cross-session • User/Session • Browser/Device • IP/Geolocation	SUSPICIOUS_BEHAVIOUR RISK_PROPAGATION USER_UNUSUAL_LOCATION USER_CHANGED_UA USER_UNUSUAL_LOCATION SESSION_CHANGED_UA SESSION_CHANGED_IP SESSION_NEW_IP ENDPOINT_NEW_ICCID ENDPOINT_CHANGED_IMEI ENDPOINT_CHANGED_UA
DEVICE INTEGRITY	• Debugging / Emulation mode • Rooted or Jailbroken	DEBUGGING_MODE DEVICE_EMULATED DEVICE_ROOTED

Figure 13. Partial list of the Cleafy's detections modules

- Use a single platform for fraud analysis by ingesting inputs from across all data sources to orchestrate centralized decisions and appropriate responses

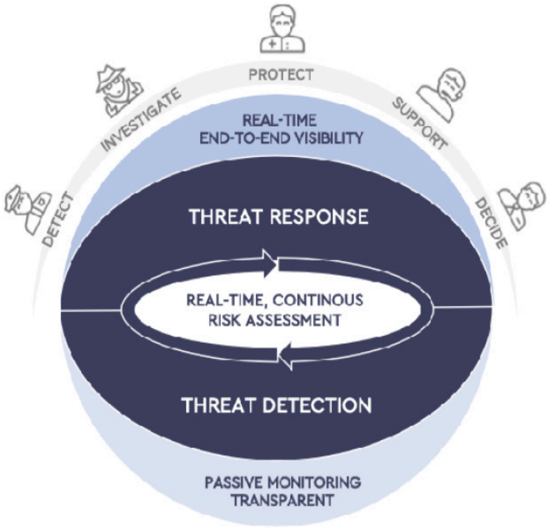


Multiple Use Cases

- Collect additional endpoints info (e.g., via grabbing JS delivered by Cleafy Platform)
- Intefrate risk score, risk factors and IOCs from external Risk Engines or other sources
- Enrich Entities (today : Sessions) with data from external sources (e.g., AssetMgmt) via custom tags

Figure 14. Example of Cleafy as Integration Hub

- Adopt a continuous and adaptive risk and trust assessment (CARTA) approach to fraud detection and prevention by moving away from a one-time risk assessment at point of login or point of payment, and instead assessing events throughout the customer journey



- Transparent, Passive Monitoring
- Deterministic Threat Detection
- Real-time, Continuous Risk Assesment
- Automated Threat Response
- Dynamic Application Protection
- Real-time, End-to-end visibility

Figure 15. Cleafy in a nutshell

Case Study Fraud Reduction

Market leader European bank offering financial services through web and mobile channels, with more that 8 million digital clients between Retail and Corporate Banking, growing rapidly on digital channels.

Scenario

The bank was expanding its digital services with a growing demand and also a clear upraise of online attacks and threats. The existing tools already deployed consisted of a transactional monitor, a biometric solution, a behavioral solution, an adaptive authentication module and a risk engine acting as orchestrator with a very strict security policy. 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 (case reviews and customer contact) and on the call center (calls from customers affected by account blocking). In terms of losses, these were increasing due to the increase in digital fraud attacks (phishing, vishing, smishing, malware) that, with the solutions deployed on silos, could not be fully detected and/or responded in time.

Proposed Solution

Cleafy offered a proof of value (PoV) covering the main application of the website part. Use cases to be covered were defined and the solution was installed, it took about 3 weeks to install and evaluate first results on real traffic. After this period and the success of the tests, the deployment of Cleafy was agreed, extending it to customer applications and the mobile channel, a working RoadMap was proposed, and in a 3 months period (from the start of the PoV to the end of the project), Cleafy team fully completed the deployment including also third party integrations such as the adaptive authentication solution and the risk engine.

Results

Cleafy, once deployed and integrated into the ecosystem, managed to provide complete visibility of customers throughout their "digital journey" by monitoring all their transactions with the bank, providing intelligence through multiple analysis (Device, Content delivered to the client versus what was sent by the backend, transactions, fingerprint, etc.), the real-time correlation of all activity in digital channels, as well as integration with third parties (adaptive authentication solution, alerting module, transaction blocking module) that enhanced its operation. All this managed to achieve the objectives detailed below:

Fraud Reduction

Cleafy achieved a **10-20% reduction in losses over existing campaigns** (types of attacks already detected by current tools) while bringing a considerable increase in the detection of new campaigns and previously undetected attacks. **Reducing the monthly open cases from 8000 to 450**, an incredible reduction over 90% such as especially advanced attacks or 'zero day' attacks (e.g., URSA malware in its development stage). This was made possible by gaining real-time device and customer visibility, which was not available with already deployed solutions, and Cleafy's multi-channel correlation capabilities (web and mobile).

Improve customer experience

Cleafy **reduced the impact on customers by 30%** on average in the first 12 months, by having a more precise risk analysis and a better correlation of information between the different digital channels (web, mobile). The blocking of transactions and clients, calls to the call center and the request for second factors in transactional operations were significantly reduced.

Increase operational efficiency

In this first year, **Cleafy decreased over 90**% the number of cases that need to be analyzed due to the improvement in customer visibility and the automation of responses. Cleafy improved reactivity and response times against fraud - early detection of fraud attacks (sometimes even prior to the fraudster 'login'), thanks to its ability to automate actions and integration with the risk engine (sending information relevant and risk score associated with the client session), the adaptive authentication module, and its ability to alert analysts to suspicious sessions for their evaluation.

Unlike other solutions, Cleafy do not require complex integrations, the PoV could be assembled within a few weeks and once in production, its simplicity made it possible to be managed by a group of 3 analysts, who in less than 3 months were able to fully manage the threat analysis and investigation activity, reducing the need to hire more people within the team to manage the increase number of threats.

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

Helping others to achieve a faster ROI

Cleafy's solution, apart from providing new capabilities, managed as well to enhance the current capabilities of existing solutions, increasing the return on investment already made in this environment.

In this case, the integration with the RSA Risk Engine managed to improve the analysis and accuracy of the risk engine, including the information from Cleafy (customer visibility in digital channels, associated risk and relevant information collected). With integration with RSA Adaptive Authentication, Cleafy risk-based second factor requests were configured when there were clear indications of suspicious sessions (early protection), even before monetary transactions occurred.

About Cleafy

We are a team of fraud hunters, cybersecurity experts, data scientists, and software engineers that since 2014 share one mission only: making technology a safer place.

Cleafy's revolutionary technology helps the largest banks and financial institutions worldwide scale-up their fight against online fraud.

A groundbreaking data-driven approach that combines the most advanced fraud detection technologies, with automated responses that stop attacks at scale. All in one central platform.

Recognized as market leader and selected vendor for Online Fraud Detection in Gartner Market Guide, we today protect over 60M+ users of top-tier retail and corporate banks.

You can visit Gartner Peer Insights to see what our customers say about working with us.

References

1. "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)
2. "Internet Threat Security Report", Symantec (2015, 2017, 2018)
3. "Net Losses: Estimating the Global Cost of Cybercrime", McAfee (2014)

Market Analysts Recognitions

Gartner

- "Market Guide for Online Fraud Detection" (G00719387), Jonathan Care, Akif Khan (May 2020)
- "Market Guide for Online Fraud Detection" (G00352548), Jonathan Care, Akif Khan (April 2019)
- "Market Guide for Online Fraud Detection" (G00318445), Jonathan Care, Tricia Phillips (January 2018)

- “Market Guide for in-App Protection” (G00368169), Dionisio Zumerle, Manjunath Bhat (July 2019)
- “Market Guide for Application Shielding” (G00317737), Dionisio Zumerle and Manjunath Bhat (June 2017)
- “Take a CARTA Approach to Building a Successful Payment Fraud Detection Strategy for Digital B2C Channels” (G00385812), Akif Khan (August 2020)
- “Take a CARTA Approach to Building a Successful Payment Fraud Detection Strategy for Digital B2C Channels” (G00385812), Akif Khan (August 2019)
- “Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats” (G00332400), Neil MacDonald and Felix Gaehtgens (May 2017)
- “Avoid Mobile Application Security Pitfalls” (G00730988), Dionisio Zumerle (July 2020)
- “Align Your Financial Fraud Detection Strategy With Gartner’s Capability Model” (G00325850), Jonathan Care and Tricia Phillips (July 2017)
- “Competitive Landscape: Threat Intelligence Services, Worldwide, 2017” (G00321925), Ruggero Contu and Lawrence Pingree (July 2017)
- Magic Quadrant for Web Application Firewalls (G00314552), Jeremy D’Hoinne, Adam Hills and Claudio Neiva (August 2017)
- “Securing Web Commerce Using PCI DSS” (G00298555), Jonathan Care (March 2016, refreshed August 2017)

Aite Group

- “Revisiting Your Authentication Control Framework “, David Mattei (December 2020)
- “Application Fraud: Accelerating Attacks and Compelling Investment Opportunities”, Trace Fooshee (November 2020)
- “The Digital Channel Under Attack: How to Protect Yourself and Your Customers”, David Mattei (June 2020)

451 Research - S&P Global

- “Cleafy sees demand for integrated fraud management for financial services”, Fernando Montenegro, Matthew Utter (March 2021)
- “Cleafy fine-tunes anti-fraud portfolio as it seeks growth in North America”, Fernando Montenegro, Matthew Utter (February 2020)
- “Cleafy takes to the cloud to reduce fraud for online businesses”, Eric Ogren (August 2018)
- “Cleafy targets website transaction fraud with web behavior analytics”, Eric Ogren (June 2017)
- “Machine Learning Signals a New Analytics Era in Security”, Eric Ogren (December 2017)

Kuppinger Cole

- “Executive View - Cleafy Advanced Threat Detection & Protection”, Alexei Balaganski (January 2020)
- “Executive View — Cleafy”, Alexei Balaganski (April 2018)

Ovum

- “On The Radar: Cleafy client-less Threat Detection and Prediction”, Rik Turner (February 2017)

Cleafy

Milan | Lubjiana | Madrid | Praha | São Paulo | Boston

cleafy.com