



# Protect on-line services and prevent frauds without impacting your users and business

Today the weakest link in the security chain is represented by the unmanaged endpoints used by your customers to access your on-line services. Advanced attacks leverage techniques such as Man-in-the-Browser (MITB), Man-in-the-Middle (MITM), Remote Access Tools (RAT) and Mobile Overlay to perform Account Takeover, Transaction Tampering and Payment Frauds.

Cleafy solution is based on innovative threat detection and threat protection technology validated by millions of customers. Cleafy makes possible to protect your on-line services and prevent frauds from compromised endpoints without impacting your users and business.

## Reduce on-line frauds

- detect advanced attacks from compromised web/mobile endpoints in real-time
- reduce customer friction by integrating any Adaptive Authentication mechanism

**Reduce frauds by up to 90%**

## Increase operational efficiency

- reduce false positives thanks to deterministic threat detection and evidence extraction
- get insights on user experience under attack and improve forensic analysis

**Shorten analysis time for case analysis from days to hours**

## Make security an opportunity

- achieve full compliance with security requirements and industry regulations (e.g. PSD2)
- apply application-transparent security without impacting your application lifecycle

**Accelerate application delivery without compromising security**

*“Cleafy continuous threat detection presents a logical approach to securing online transactions as fraud rates, particularly those driven by automated software bots and based on advanced techniques, relentlessly climb. Cleafy also provides unique threat protection capabilities that enhance safe transactions from infected endpoints.”*

*- Eric Ogren, Senior Security Analyst, 451 Research*

# Cleafy delivers client-less and application-transparent threat detection and protection for your on-line services



## Advanced threat detection and protection

- Patented Full Content Integrity (FCI) continuously verifies full application integrity (DOM/XHR/API)
- Deep threat visibility automatic extraction of threat evidence (e.g. malicious web-injects and mobile apps)
- Patented Dynamic Application Encryption (DAE) to enable safe transactions from infected endpoints



## Client-less and application-transparent

- Client-less - no agent deployed and passive mobile SDK – no touch of application backend infrastructure
- User-transparent – no impact on end-user experience, content delivery and endpoint performance
- Application-independent - no changes required to application code – no re-training upon new releases



## Open, scalable and cloud-ready

- Open architecture and comprehensive REST APIs –integrates any Transaction Monitor, Case Mgmt, SIEM
- Scalable to continuously monitor full application perimeter and analyze millions of events / day
- Deployed either on-premise or over the Cloud

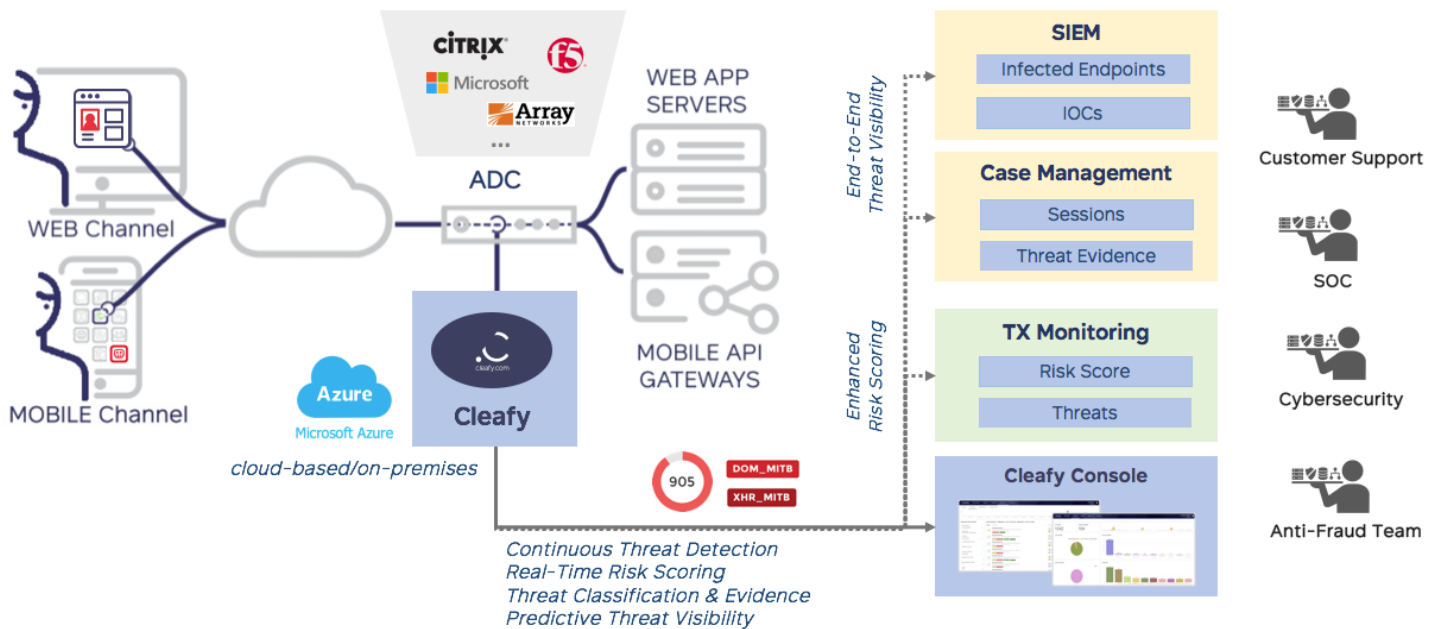
## Our promise to you

Cleafy will provide measurable benefits: unparalleled end-to-end visibility, real-time detection of advanced threats, ability to discover anomalous behaviors, identify attack patterns and predict evolution of attack campaigns, activate automated threat response actions and dynamic threat protection mechanisms

## An offer to get you started

Get in touch with us at [info@cleafy.com](mailto:info@cleafy.com):

- Verify how smoothly Cleafy can be integrated in your architecture without any change to your web/mobile apps
- Learn how easily Cleafy can be adopted in your environment and immediately provide its benefits
- Discuss the available options to quickly validate Cleafy technology in a POC



## About Cleafy

Cleafy delivers innovative fraud prevention solutions based on patented threat detection and protection technology. Cleafy solutions provide adaptive, continuous, user-transparent and application-independent security.

Cleafy has been successfully adopted by millions of users of leading corporate and retail banks to prevent on-line frauds while reducing customer friction, improve overall security posture and operational efficiency of security teams.