Kaspersky Fraud Prevention Cloud

Attacks KFP fights

The system is capable of detecting attacks that target either user accounts or banking sessions, such as:

Account Take Over – when stolen credentials are used to access accounts.

New Account Fraud – when new accounts are created to commit fraud.

Phishing / pharming – when fake sites are used to steal sensitive information such as PII, credentials, etc.

Bots / card testing / cross-checks – when a fraudster is a machine, not a human.

RAT attacks – attacks that utilize RAT capabilities to gain access to a device used for banking, in order to commit fraud.

Web-injects – attacks that use the web injection method to add extra fields to a bank's online login page.

Feature List

Feature	Description	Release
Risk Based Authentication (RBA) for online and mobile channels	Aimed at assessing the risk for a login (before a user is allowed into the OBS), with the purpose of improving usability for honest users by decreasing the number of frictions (additional authentications) and the detection of risky logins, as follows: Green – allow login into OBS without any second factor authentication. Grey – request additional authentication info. Red – forbid access / restrict functionality, contact the customer for further verification.	•
Continuous Session Anomaly Detection	Provides continuous assessment of the session risk, based on user behavior analytics, device reputation, biometry data and more (the full range of detection technologies is described in the table below). The bank's anti-fraud analysts are alerted if any abnormal behavior is detected. This significantly empowers the internal transactional monitoring systems, providing the means of early detection and automation, and increasing the detection rate. Risky transactions are the subject of high attention and manual processing while honest ones can be processed automatically without any delays.	•

Feature	Description	Release
Cross-channel Fraud Detection	The detection of fraud attacks at account level across mobile and online channels. Analyzes the combination of parameters and events from all user devices used as touch points to access accounts in the OBS and makes decisions based on the overall reputation of devices and accounts over time. This thorough analysis of data gathered from all devices and channels allows for the efficient detection of complex fraud attacks at account level as well as helping to constantly improve detection accuracy. This, in turn, decreases false alarms and friction for honest users.	2017
Fraud incubation period detection	When it's not yet a fraud attack but preparation activities are underway. These can include logging into an OBS to harvest a victim's personal data and creating "good" transactions to abuse transaction monitoring systems. This helps a fraudster earn a good reputation for a device / user that will later be used to conduct attacks, etc.	2017
Comprehensive Reporting	**Incident dashboard:** An interactive graphic user interface, in a cloud console, allows a bank's anti-fraud analysts to access information on any fraud detected. The console capabilities include incident monitoring, viewing system activity reports and feeding the machine-learning system with information about the fraud detected. **Thorough investigation:** Incident investigation and digital forensics – these reconstruct a detailed picture of any incident using comprehensive reports, including incident remediation steps.	•

Detection Technologies

Feature	Description	Release
	Device and Environment Analysis	
Global Device Reputation	Provides the reputation of the device, leveraging the power of global Kaspersky Lab intelligence, based on information from millions of users all over the world. Reputation is based on both tag and tag-less fingerprints.	•
Emulators and odd devices detection	Detection of suspicious devices, device emulators and device configurations that are usually involved in fraud.	•
Global IP reputation	Provides the reputation of IP addresses based on Kaspersky Lab global presence and knowledge that helps to identify connections from suspicious IP addresses.	•
TOR detection	Detection of a TOR browser using IP intelligence in combination with device analysis.	•
Proxy detection	Detection of a connection from an anonymized proxy using IP intelligence in combination with device analysis.	2017
	Behavioural Analysis	
User and population behavior patterns	Analyzes navigation behavior for each user's activity against user, population and known fraudsters' patterns.	•
Bots detection	Detects automated tools and robot behavior.	•

Feature	Description	Release
Clientless Malware Detection*		
Direct detection	Detects the protected banking web page modification. This technique is valuable in detecting whether the user's device is infected with malware that is already known to be directly targeting your digital banking services.	•
Proactive detection	Proactively helps to detect whether a user's device is infected with malware that is targeting other banks – these users can be selected as 'high risk' as that malware may later be adapted for use in targeting your bank.	•
Behavioural Biometrics		
Passive Biometrics	Detects whether the device is under the control of a legitimate user or not. Analyzing mouse movements, clicks, scrolls, keystrokes, etc. – on a PC; and analyzing all types of sensor events – accelerometer, gyroscope, and all possible types of gestures (touch events, swipes etc.) – on mobile devices.	•
RAT detection	Detection of connections from remote administration tools.	•
Human Intelligence		
FraudDetection-as-a-service	Kaspersky Lab's dedicated Fraud Analysis Group provides constant support to our clients. We provide expertise on cybersecurity issues and incident response services for highly complicated cases of fraud attacks. This expertise is continuously feeding our cloud services, improving them and keeping up ready to fight new threats.	•
24x7 support	Corporate support for our cloud services, ensuring the stable provisioning of security to our clients.	•

* Optional feature, requires on-premise installation.

All about Internet security: **www.securelist.com**
Find a partner near you: **www.kaspersky.com/buyoffline**

www.kaspersky.com
#truecybersecurity