Kaspersky Fraud Prevention Cloud

Proactive Account-based Fraud Protection for Web and Mobile Channels

Customer devices you don't control sit beyond your security perimeter and are likely under- or even un-protected. Regardless, they are routinely granted access to your sensitive digital banking applications and allowed to perform a variety of high risk activities. As most customers use multiple channels to access your banking applications, it becomes challenging to have ultimate confidence that your financial institution has adequately established protection strategies for them all.

The Expanding Attack Surface and the Need for an Account-Centric & Multi-Channel Fraud Prevention Approach

Additionally, fraudsters often attack one channel in order to facilitate cross channel fraud (for example: attacking relatively unsecured mobile banking credentials to log into online banking applications to commit account takeover). This leads to the inevitable conclusion that there is a need to protect the account holistically, not just the device or individual channel. This strategy requires an account-centric & multi-channel approach.

Kaspersky Fraud Prevention Cloud is capable of detecting attacks that target either user accounts or banking sessions, such as:

- Account Takeover
- New Account Fraud
- Phishing / Pharming
- Bots / card testing / credential cross-checking
- Attacks with Remote Administration Tools
- Man-in-the-Browser attacks

Kaspersky Fraud Prevention Cloud analyses the combination of parameters and events from all user devices used to access accounts.

Makes decisions based on the overall reputation of devices and accounts over time.

Allows for the efficient detection of complex fraud attacks at account level as well as helping to constantly improve detection accuracy.

Kaspersky Fraud Prevention Cloud combines 4 key fraud prevention technologies based on Machine Learning algorithms:

- **Clientless Malware Detection** checks if the customer's machine is infected with malware without additional software on the user's side. This data is used for risk based authentication and machine learning modeling, and to determine the legitimacy of transactions.
- **Behavioural Biometrics** analyses unique customer's interaction with device, such as mouse movements, clicks, touches, swipe speed and more to detect whether a device is being used by a legitimate user or not. This technology detects bots and remote administration tools.
- **Behavioural Analysis** analyses what the user clicks, how he acts during the session and login. Also looks at the typical navigation and time patterns and other aspects. This allows a profile of normal behaviour to be built and any abnormal or suspicious activity.
- **Device and Environment Analysis** leverages the global presence of Kaspersky Lab to identify "good" devices and use this knowledge for user authentication. Based on global device ID, IP-address, location reputation and more, any attribute marked as involved in fraudulent activity is also proactively detected and shown as suspicious or related to fraud.

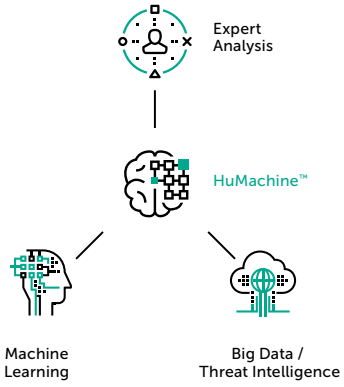
Machine Learning methods, being the core part of the system, enhance the key technologies activating additional components of fraud detection:

Risk Based Authentication (RBA) makes it possible to dynamically assess the risk level when a user logs in to the system. Based on this assessment and real-time verdicts from Kaspersky Fraud Prevention Cloud, your organisation can make a decision on how the transaction should be processed further: allow access, request additional authentication or restrict available services. This brings fraud detection to a new level, providing real-time responses and avoiding additional authentication steps for legitimate customers .

Continuous Session Anomaly Detection provides continuous assessment of the session risk, based on the analysis of behaviour, device and environment, biometric data and more. This significantly empowers internal transaction monitoring systems, providing the means of early detection and automation, and increasing detection rate. Risky transactions can be made the subject of high attention and manual processing while legitimate ones can be processed automatically without any delays.

Kaspersky Fraud Prevention Cloud does not replace your internal monitoring solution. Instead, it complements it by constantly providing your teams with data, necessary for real-time detection of fraudulent activity before a transaction occurs. This empowers your current systems to benefit from additional and proactive context for quicker and more accurate decision-making, as well as for intelligent and adaptable use of step-up authentication.

Contact us to learn more: kfp@kaspersky.com



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

www.kaspersky.com
#truecybersecurity