Kaspersky Fraud Prevention

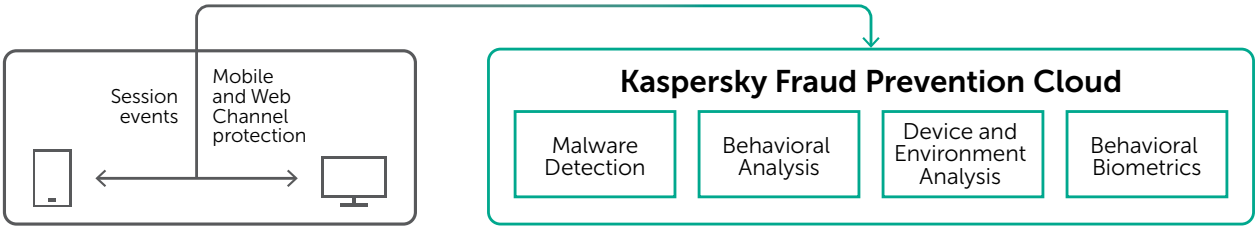
Ready for GDPR

Advanced technologies for real-time cross-channel fraud detection

Businesses have already gone far beyond traditional services providing their customers with access to their personal accounts via online channels and mobile devices. Digital transformation brings new opportunities, customers and of course, more revenue. On the other hand, it opens the doors to fraudsters with new sophisticated schemes, cross-channel attacks both on the user's device and account.

New Account Fraud	Account Takeover	Tools for Fraud Automation
Money Laundering and Loyalty Fraud	Attacks with Remote Administration Tools	Malware and Phishing

Kaspersky Fraud Prevention uses a complex range of advanced technologies with Machine Learning applied for proactive detection of sophisticated fraud schemes across web and mobile channels, in real-time, before the transaction occurs.

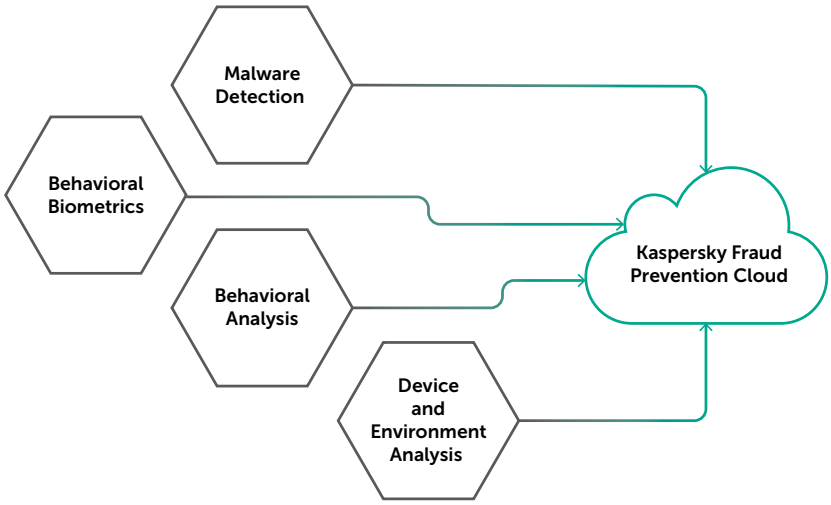


Device and Environment Analysis leverages the global presence of Kaspersky Lab to identify "good" devices and use this knowledge for user authentication. Based on global device ID, IP-address, location reputation and more any attribute marked as involved in fraudulent activity is also proactively detected and shown as suspicious or related to fraud.

Behavioral Analysis looks at the user's activity during the login and session, analysing the typical navigation and time patterns, how the user acts in the personal account, what he clicks and more. This data allows profiles of normal behavior to be built and any abnormal or suspicious activity during the login and the whole session to be detected.

Behavioral Biometrics analyses your unique customer's interaction with their device, like mouse movements, clicks, touches, swipe speed and more to detect whether a device is being used by a legitimate user or not. This technology can also be used to detect bots and remote administration tools.

Malware Detection is checking if the customer's device is infected with malware covering both web and mobile channels. The technology is using several sophisticated approaches including non-signature detection and agentless availability.



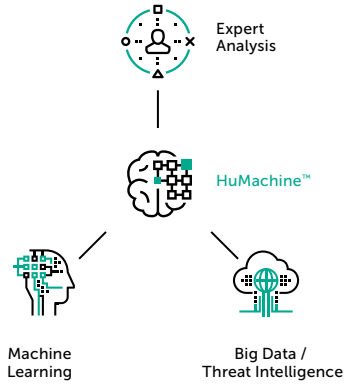
Machine learning is the core part of Kaspersky Fraud Prevention Platform. Various machine learning methods based on supervised and semi-supervised approaches are applied to enhance the efficiency and accuracy of Kaspersky Fraud Prevention Technologies.

Depersonalised data processed by 4 key technologies turns into real-time verdicts within Kaspersky Fraud Prevention Cloud. Based on continuous and proactive analysis of device and session reputation across online and mobile channels, behavioral and biometric data and other aspects, our Cloud solution feeds your internal monitoring systems with data crucial for timely and highly efficient fraud detection. This empowers your current systems to benefit from the additional context for proactive and more accurate decision-making, as well as for intelligent and adaptive use of step-up authentication.

KEY BENEFITS:

- Continuous and proactive real-time detection of advanced fraud before transaction occurs
- Multichannel fraud detection: online and mobile channels
- Detection of fraudsters and money laundering
- Improved user experience due to RBA, leading to growth and retention of customer base
- Comprehensive session statistics for forensics with dedicated team support
- Complements existing Enterprise Fraud Management solutions
- Productivity improvements with automation

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