Kaspersky Fraud Prevention

Ready for GDPR

Kaspersky Advanced Authentication

Digital is taking over the world. Millions of users globally are choosing PCs, tablets and mobile phones to get access to services and personal accounts. One of the crucial business tasks now is creating conditions for clients:

- Fast and seamless access to the personal account
- Preferable and handy authentication methods
- Confidence in safety of the services used.

Advanced Authentication knows who is using your services in web in mobile channels: a legitimate user or a fraudster, a human or a bot.

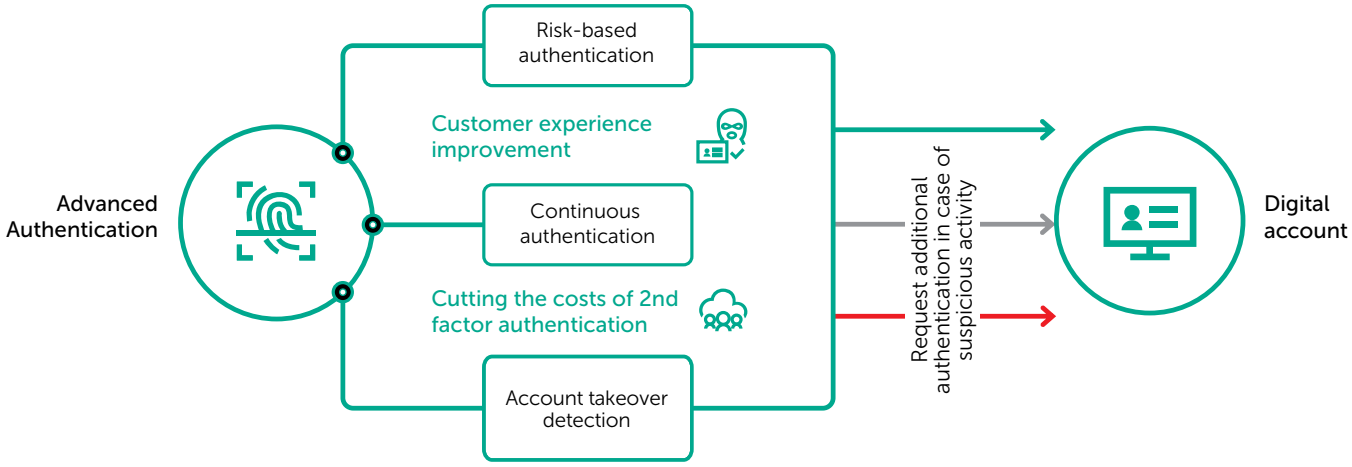
Analysis of behavioral data, passive biometrics as well as device and environment around it result in objective risk assessment. The weighted analysis of hundreds of unique parameters from the beginning of the session provides a balanced estimation with certain outcomes:

- Legitimate users get rid of annoying and unnecessary authentication steps
- Suspicious users are eligible for additional verification
- The most suspicious activities are subject to strong verification with possible restriction of access

Advanced Authentication is made to improve the user experience, cut the costs of second factor authentication and continuously detect suspicious activity leading to business growth and higher level of security.

Functional components of Advanced Authentication

Risk-Based Authentication eliminates additional authentication steps for legitimate users letting them into the session without unnecessary frictions. Continuous analysis of hundreds of parameters in real-time enables the dynamic risk assessment allowing you to make a fast and accurate decision regarding the level of access you grant to your users. Moreover, the RBA can functionally detect signs of Account takeover at an early stage. Thus, actions different from the behavior of a legitimate user based on a number of indicators are considered to be potentially fraudulent and are subject to additional verification.

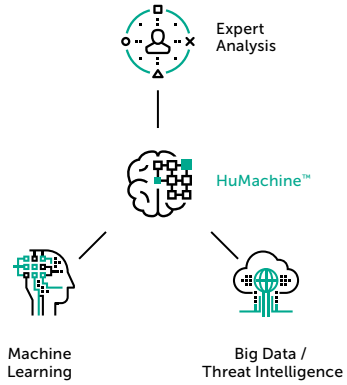


Key Benefits of Advanced Authentication

- Seamless user experience for your clients
- Cutting the costs of 2nd factor authentication
- Detection of Account takeover at an early stage
- Helps act in accordance with local compliance

Continuous Authentication provides the higher level of security during the whole session. It is analyzing behavioral and biometric data, device reputation and other valuable non-personalized information that is coming to Kaspersky Fraud Prevention Cloud. In case of any signs of abnormal or suspicious behavior Advanced Authentication automatically sends appropriate verdicts to authentication services to request the second factor and stop potentially illegal use of the personal account.

Account Takeover Detection enabled by Advanced Authentication allows you to know who is standing beyond the device: a legitimate user or a fraudster. The solution is able to identify new devices with unique extended device fingerprinting functionality. Additionally, the real-time analysis of behavioral and biometric data determines deviations from the typical user behavior. The timely detection of compromised account significantly reduces potential financial losses both for businesses and for the users.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/fraudprevention**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

kfp@kaspersky.com