Beat fraud and ensure seamless digital experience for your customers

Kaspersky Fraud Prevention

kaspersky BRING ON THE FUTURE

Find out more at kfp.kaspersky.com

Preventing cross-channel cyberattacks in real time

Businesses have already gone far beyond traditional services, providing their customers with access to their personal accounts via online channels and mobile devices. On one hand, 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 and cross-channel attacks both on the user's device and account.

Kaspersky Fraud Prevention processes traffic in real time according to the following parameters:

Metric name	Number of unique units per day
Device	~50 M
User	~29 M
Online session	~332 M
Processed event	~6 Bn

Session events analysis with Kaspersky Fraud Prevention

Device and environment analysis

Leverages the global presence of Kaspersky 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, remote administration tools and early signs of account takeover.

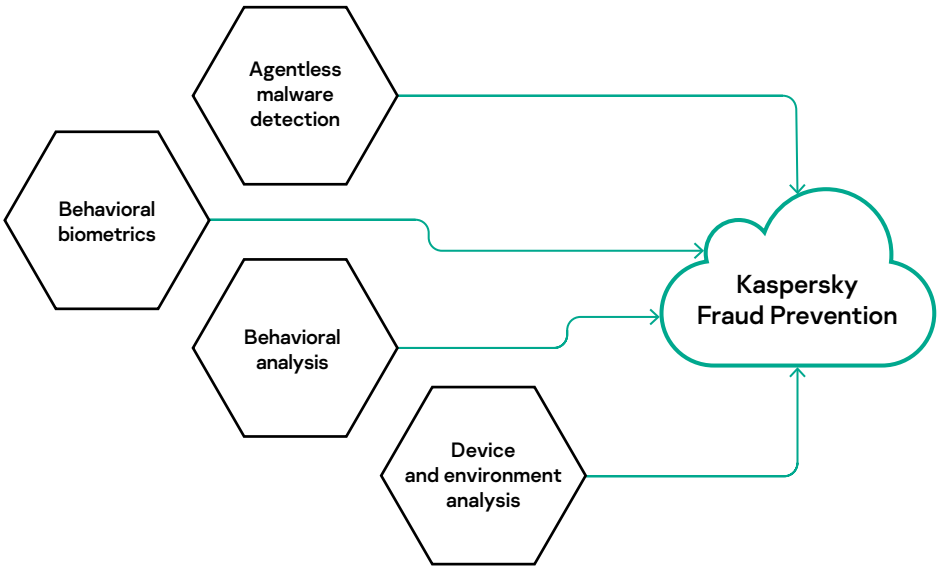
Malware detection

Helps determine whether the customer's device is infected with malware covering both web and mobile channels without any additional components having to be installed. The data about a possible malware infection is used for Risk-Based Authentication (RBA), as well as determining the legitimacy of transactions.

Depersonalised data processed by 4 key technologies turns into real-time verdicts within Kaspersky Fraud Prevention.

Based on continuous and proactive analysis of device and session reputation across online and mobile channels, behavioral and biometric data and other aspects, our solution feeds your internal monitoring systems with data crucial for timely and highly efficient fraud detection. This empowers your current systems to detect automation tools, bots, suspicious user behavior, a multitude of globally used malware and other tools used for fraud.

The ready-to-use incidents generated by Kaspersky Fraud Prevention allow for proactive and more accurate decision-making, as well as for intelligent and adaptive use of step-up authentication.

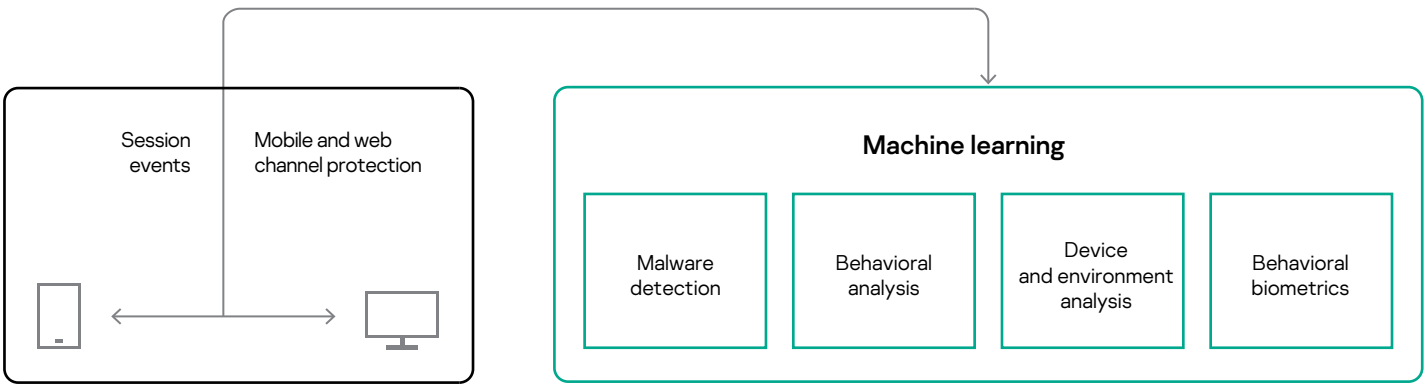


Key technologies used by Kaspersky Fraud Prevention

Key benefits of Kaspersky Fraud Prevention

- Continuous and proactive real-time detection of advanced fraud schemes before transactions occurs
- Multichannel fraud detection: Web and mobile channels
- Detection of fraudsters and money laundering schemes
- Improved user experience through Risk-Based Authentication, leading to growth and retention of customer base
- Comprehensive session statistics for forensics with dedicated team support
- Compliments existing Enterprise Fraud Management solutions
- Productivity improvement and reduced operational costs through automation and machine learning

Machine learning is the core part of the Kaspersky Fraud Prevention Platform. Various machine learning methods, such as clustering, neural networks and decision trees, all based on supervised and semi-supervised approaches are applied to enhance the efficiency and accuracy of Kaspersky Fraud Prevention Technologies. This allows for next-level fraud prevention throughout the entire session, before any transactions occur. At the same time, trough **Risk-Based Authentication (RBA)**, legitimate users can skip additional authentication steps and access their accounts without any inconvenience.



Automated Fraud Analytics

Implementing a security strategy is not only about the cutting-edge technologies. It's about the data you get during the analysis of the user session and the ability to use it along with technologies.

That's what Automated Fraud Analytics is created for: to make sure you know about the possible fraudulent activity when it has not started yet, have all the data and analysis crucial to make accurate and timely decisions and uncover complex fraud cases.

Use cases

Incidents generated by Kaspersky Fraud Prevention

- Infected device **63%**
- Account takeover **34%**
- Money laundering **3%**
- Automation tools **0,39%**
- New account fraud **0,14%**

Account takeover. What if you knew who is beyond the device in your digital channel? What if you knew how the user behaves in the digital journey? That's what we look at with Kaspersky Fraud Prevention. We help you learn more about your customers, providing you with valuable data and knowledge to see the anomalies and suspicious behavior before fraud has even been committed, while ensuring that your valued customer doesn't unnecessarily lose access to their account.

New Account fraud. To protect your organization from New Account fraud, Kaspersky Fraud Prevention applies core technologies like behavioral biometrics and analysis, as well device and environment analysis, to build patterns of good and bad behavior. The solution is able to identify accounts specially created to commit fraud: steal miles, generate bonus points and bring harm to business.

Money laundering. With entity-linking functionality and device fingerprinting, Kaspersky Fraud Prevention reveals groups of accounts accessed from one PC or mobile device. Behavioral analysis enhances the detection rate meaning good users can be separated from fraudsters. Thanks to global device reputation, Kaspersky Fraud Prevention also detects links between money mules across companies stopping cross-organizational fraud schemes.

Fraud Intelligence – throughout the whole session, all of the events happening around the users, their devices, biometric and behavioral peculiarities and deviations are thoroughly analyzed. Access to session events allows to find various kinds of suspicious activity such as remote administration tools, bots, malware and many others. Combination of technologies and expertise makes it possible to customize the solution for the business needs, and thoroughly investigate the detected cases of fraud.

Threats

- **Fraud on the rise** – growing customer concerns
- **Higher fraud level** – risk of regulatory fines
- **Missing the attack incubation stage**
- **Emerging complexity of attacks** – legacy solutions are not enough

Functional capabilities

- Automated global entity **linking and mapping**
- Deep-learning-based **behavioral analysis**
- **Flexible** rules engine **configuration**

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 great user experience for clients:

- **fast and seamless access to the personal account;**
- **convenient authentication methods;**
- **confidence in the security of the services used.**

Advanced Authentication knows who is using your services in web and 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.

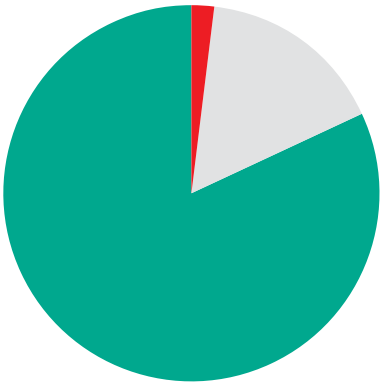
Advanced Authentication provides a high level of security throughout the session thanks to **continuous authentication and anomaly analysis**. The solution evaluates data on user behavior, device reputation and other information already accumulated by Kaspersky Fraud Prevention.

If anomalous behavior is detected, the solution automatically submits data about it to internal monitoring systems, and uses the authentication system to request a second factor and determine the legitimacy of the transaction and the user.

Based on the processing of depersonalized data and automatic information analysis, Advanced Authentication is capable of detecting **account takeover**. The solution is able to identify as well as discover new and previously unused devices by using unique fingerprinting. In addition, real-time behavioral and biometric data analysis detects deviations from «typical» user behavior.

Both during the login phase and during the session, early detection of compromised accounts makes it possible to limit the level of access to personal accounts and reduce potential financial losses to businesses and clients.

Risk-Based Authentication verdicts



- Red (high risk of fraud) **1,95%**
- Gray (not enough information, moderate risk of fraud) **16,21%**
- Green (legitimate user) **82%**

Functional components of Advanced Authentication

Risk-Based Authentication (RBA) 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 second factor authentication
- Detection of account takeover at an early stage
- Helps act in accordance with local compliance

What is great authentication?

Legitimate user

It might be quite annoying for a legitimate user to receive an SMS with a code every time they try to access their digital account.

Second factor authentication

- SMS
- E-mail
- Call

Digital account

For a business, adding second factor authentication would make user experience onerous and would create a risk of losing clientele.

Basic second factor authentication process

- Disrupts the session
- Takes more time
- Second factor can be stolen

Nevertheless, a balance between secure authentication process and seamless customer experience is key to making both parties content with the service.

Risk Based Authentication

Additional verification is only required when the risk score is higher than usual. That means frictionless access for proven customers and restricted or denied access for fraudsters. Numerous unique parameters are monitored in order to detect suspicious activity and estimate risks.

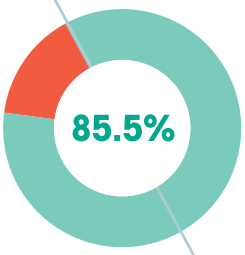
User gets benefits

- Seamless interaction with the service
- Faster transactions and purchases
- Higher level of data protection

Business gets more efficient

- True machine learning
- Forensic capabilities
- Reduced operational costs

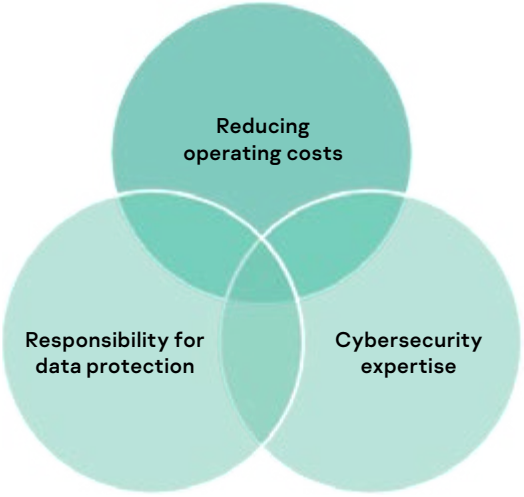
85.5% of users get to their accounts without additional verification according to Kaspersky Fraud Prevention statistics.



Numerous unique parameters are continuously monitored in real-time by RBA

- User behavior
- Geolocation
- Login time
- Biometrics
- Usual device used
- 40+ more unique parameters

What do Fraud Prevention and Managed Security have in common?



Companies believe that MSSP (Managed Security Service Provider) services can help reduce their security costs. They look to outsource the entire IT infrastructure, including security, because they lack the internal resources and necessary expertise.*

* Source: Global IT Security Risk Survey 2017

A wider range of services in conjunction with Kaspersky Fraud Prevention

Increasing revenue

- Broader client coverage through enhanced authentication, fraud detection and incident investigation.
- Flexible, scalable business model allows you to quickly adapt to customer requirements.
- Integration of cloud, private cloud or on premise depending on customer preferences.

Sales support

- Marketing materials.
- Partial refund of invested funds and rebates.
- Joint sales programs.
- Training opportunities for technical and sales specialists.

An extra level of protection

- Advanced Authentication as part of an extended package for the online channel of a company.
- Monitoring and analysis of customer sessions in online service channels.
- Machine learning capabilities.

Customer package including forensics and analysis in the field of cyberfraud

- Detecting and monitoring is often not enough to prevent future attacks. Analysis is a mandatory feature to prevent fraudulent attacks before any damage is caused.
- Kaspersky's research and analysis team draws on more than 22 years of experience in the field of cybersecurity and is always ready to conduct in-depth investigations into detected cases of fraud and anomalies.

kaspersky BRING ON THE FUTURE

Beat fraud. Ensure seamless customer experience.

Kaspersky Fraud Prevention

We strive to help businesses on the global arena proactively prevent fraud and deliver a smooth customer experience through the use of innovative fraud detection technologies.

Benefits

- Cutting operational costs
- Uncovering crossorganizational money laundering schemes
- Improving the user experience
- Thorough and extensive fraud analysis

kfp.kaspersky.com
@KasperskyFP

IT security news:
www.kaspersky.com/blog
Cyber threats news:
www.securelist.com

Kaspersky Fraud Prevention is rated 4.9 on Gartner Peer Insights: https://www.gartner.com/reviews/market/online-fraud-detection-systems/vendor/kaspersky/product/kaspersky-fraud-prevention

www.kaspersky.com

WORLD BRANDING AWARDS BRAND OF THE YEAR