

KASPERSKY BRAND MONITORING

PRODUCT TERMS AND CONDITIONS

These Product Terms and conditions ("Product T&C") set out the special terms and conditions applicable to Kaspersky Brand Monitoring and are to be read in conjunction with the [Kaspersky Threat Intelligence Agreement](#) ("Agreement"), that applies to these Product T&C.

These Product T&C are legally binding and govern Customer's and Partner's use of Kaspersky Brand Monitoring ("Product"), accordingly Kaspersky advises to read them carefully.

By purchasing, accessing and/or using the Product, and/or by clicking the appropriate acceptance button if required by Kaspersky (which shall, to the maximum extent permitted by applicable law, constitute conclusive acceptance thereof), Customer or Partner accepts and agrees to be bound by these Product T&C and shall ensure that all individuals or legal bodies involved in purchasing, accepting and using the Product are aware of the terms of these Product T&C and should comply with the same.

By accepting the Product T&C on behalf of Customer or Partner, You represent and warrant that,

- (i) You have full legal authority to bind Customer or Partner to the Product T&C accordingly;
- (ii) You have read and understand these Product T&C;
- (iii) You agree, on behalf of Customer or Partner accordingly, to these Product T&C.

In the event of any conflict between the provisions of these Product T&C and any separate agreement entered into between Kaspersky and the Customer or Partner, the terms of such separate agreement shall prevail only as expressly stated therein. These Product Terms supplement the separate agreement and take precedence over any Customer/Partner purchase order or similar document.

1. DESCRIPTION

Kaspersky **Brand Monitoring** is a comprehensive cybersecurity practice designed to detect and mitigate brand abuse, impersonations, and other online threats. Kaspersky's solution combines advanced monitoring tools with best practices to safeguard Customer brand's reputation, protect digital assets, and ensure the safety of Customer clients and employees.

Features

Product provides:

- **Phishing and Scam Monitoring:** Identifies phishing web resources and scam resources such as domains and URLs, Cybersquatting (TLD, typo-squatting, combo-squatting) domains.
- **Social Networks Monitoring:** Identifies fake profiles, accounts and groups, impersonating Customer's brand on platforms like Facebook, Instagram, Telegram, and X(Twitter).
- **Mobile Marketplaces Monitoring:** Detects fake or rogue mobile applications on Google Play and the App Store that misuse Customer's brand.
- **Threat notifications:** reporting in the form of threat notifications via the Kaspersky TIP or API to keep the Customer informed about threats.

Benefits

Product provides actionable insights and recommendations to protect Customer's brand from online threats. Product offers:

- **Protects Customer's brand** - Product protects Customer's reputation by monitoring of the unauthorized use of its brand or intellectual property online. This helps prevent damage caused by fraudulent activity, such as brand impersonation, phishing and scams.

- **Protects Customer clients' trust** - Clients rely on brands as a sign of trust and quality. By protecting the brand, Product helps to maintain clients' trust and significantly reduces the risk of being misled or deceived by fraudulent activities.
- **Delivers a competitive advantage** - A company that proactively protects its brand is more likely to be seen as trustworthy and reliable, establishing a significant competitive advantage.
- **Protects Customer's revenue** - A damaged brand reputation can lead to reduced revenue due to loss of clients' trust and loyalty. Product helps to prevent revenue loss caused by brand damage, by protecting Customer's brand.
- **Supports compliance** - Companies operating in certain industries, such as finance and healthcare, are required to comply with strict regulations to protect sensitive client's data. Failure to comply with these regulations can result in hefty fines and legal liabilities. Product supports compliance with regulatory requirements.

Product is powered by a combination of automated tools, machine learning algorithms, and manual analysis to ensure comprehensive coverage and accurate threat detection.

Phishing and Scam Monitoring

Product employs domain monitoring tools, web crawlers and KSN sensors to detect phishing websites and typo-squatting domains. The process includes:

- **Domain Registration Monitoring:** The system monitors newly registered domains for variations of Customer's brand name or trademarks.
- **Phishing Analysis:** The system detects phishing resources based on the analysis of KSN sensors and partner data.
- **Content Analysis:** Product uses machine learning algorithms to analyze website content for phishing indicators, such as fake login pages or fraudulent forms.

Key Features:

- Detection of phishing/scam web resources.
- Identification of typo/combo-squatting domains (newly created).
- Comprehensive reporting in the form of threat notifications on the Kaspersky TIP to keep Customer informed about threats.

Social Networks Monitoring

Product employs web crawlers with major social network platforms to scan for fake profiles, accounts and groups impersonating Customer's organization. The monitoring process includes:

- **Profile Analysis:** Using natural language processing (NLP) to detect impersonations.
- **Keyword Tracking:** Product tracks specific keywords, and mentions related to Customer's brand to detect misuse or impersonation attempts.

Supported Platforms:

- Facebook
- Instagram
- Telegram
- X(Twitter)

Mobile Marketplaces Monitoring

Product uses automated scanning tools to monitor mobile app official marketplaces for fake, or rogue applications. The process includes:

- **App Metadata Analysis:** The system analyzes app names, descriptions, and developer information to detect apps misusing your brand.

Supported Platforms:

- Google Play
- App Store

Assets

In order to continuously monitor and analyze Customer's organization digital footprint, and to identify cybersecurity threats, Kaspersky experts work with 'Assets'. These are indicators associated with Customer's organization and may take a number of forms, including:

- Company/brand name
- Domain
- Keywords
- Mobile app link
- Social Networks account link

Assets can be added by Customer, or by Kaspersky experts at any time. Customer can request removal of Assets at any time. Customer can also specify *exceptions* – specific objects for which Kaspersky experts will not do searching. Number of assets is stated in the Order, and the related Certificate.

Information about each asset is displayed on the **Digital Footprint** → **Asset management** page of Kaspersky TIP, as shown in the table below.

Field	Description
Asset	Asset included in or excluded from the research.
Category	Available values: • Company/brand name – Customer company or brand name. • Domain – Domain or subdomain name. • Keywords – Keywords to search in Surface Web. • Mobile app link – Link to the actual and legitimate page of the Customer's mobile application in a supported application store, using the Customer's brand used in the work. • Social Networks account link – Link to the actual and legitimate page of the Customer's social network account in a supported social network
Status	Available values: • Sent for validation – Asset is in process of being validated by Kaspersky experts. • Confirmed – Asset is confirmed by Kaspersky experts. • Rejected – Asset is rejected by Kaspersky experts.
Inclusion	Indicator of the asset's inclusion in the research. Available values: • Included—Asset is included in the research. • Excluded—Asset is excluded from the research.

Status details

Comment for the asset's status. Available only for assets with **Confirmed** or **Rejected** status.

Customer grants Kaspersky a worldwide, royalty-free license to use submitted Assets solely for Product delivery. Threat Notifications and intelligence remain Kaspersky's exclusive IP. Customer may not: (i) resell data; (ii) create derivative works; or (iii) use for competing services. Kaspersky may reject Assets at its discretion.

Managing Threats

Customer can change a notification state, assign it to a certain User, and add a comment.

Dashboard

- **Threats** — Summary for threat notifications:
 - **Select the time period** — allows to select the time period to filter the displayed threat information for a specific period. “**No data found**” is displayed, if there are no any threat notifications about the threats for the selected period.
 - **Distribution of threats by category** — threat categories for the selected period sorted by number of threat notifications in each category, in descending order.
 - **Threats by notification date** — graph of the threat notifications by date when they were received. Graph is displayed for the selected period.
- **Assets** — Summary for assets:
 - **Distribution of Assets by status** — total number and proportion of assets with different verification statuses.
 - **Distribution of Assets by source** — total number and proportion of asset sources (added by Users or Kaspersky experts).
 - **Distribution of Assets by category** — asset categories sorted by number of assets in each category, in descending order. **No data found** is displayed, if Customer does not have any submitted assets.

Threat notifications

Threat notifications provide information about detected unauthorized use of Customer's brand or intellectual property, as well as any other fraudulent activities that may harm Customer's reputation.

These notifications may include information about fake social media accounts and applications, phishing websites, and other fraudulent activities that can damage company's reputation and/or deceive clients.

Real-time Threat notifications will be delivered to the Kaspersky TIP. Kaspersky TIP provides:

- **Dashboard:** A centralized view of all detected threats, including social media impersonations, fake apps, phishing domains.
- **Threat Notifications:** Real-time alerts for new threats.
- **API Access:** The Product offers RESTful API access, allowing Customer to integrate threat data into its existing security systems and workflows.

Product Options

Purchased License provides access to the Product, available on the Digital Footprint Tab of the Kaspersky TIP.

Product provides Threat notifications and Assets management of the supported types:

- o Domains
- o Company/brand name
- o Social Networks Links
- o Mobile Apps Links
- o Keywords
- o Phishing
- o Typosquatting
- o Fake application
- o Fake social media entity

The number of Assets is limited by the Product option and is stated in the Order and the related Certificate.

Access to the features on Kaspersky TIP is available for the Customer only (not to subsidiaries, affiliates or other related organizations).

Number of the Customer accounts, registered in the Kaspersky TIP is unlimited.

In addition, Kaspersky provides access to Kaspersky Threat Lookup, limited by fifty (50) searches per day, as a part of the Product.

The type and prices of the Product are indicated in the Proposal, and/or in the Kaspersky's price list in effect at the time of Order placement, which Customer or Partner declares to know and accept; and the current price list shall supersede all previous price lists.

License may be purchased for different Subscription Periods.

Kaspersky provides Product option(s) in accordance with the Order, the Certificate and these Product T&C.

2. DELIVERY

2.1. License. Kaspersky grants Customer or Partner a non-exclusive, non-sublicensable, non-transferable, limited license to access the Kaspersky Threat Intelligence Portal ('Kaspersky TIP') solely to: (i) add Assets; (ii) receive Threat Notifications; and (iii) use associated APIs strictly in accordance with documentation provided by Kaspersky. This license is limited to the number of Assets and Subscription Period specified in the Order/Certificate. No right to extract, republish, or commercially exploit Threat Intelligence data is granted.

2.2. Trial Use License. Kaspersky grants Customer or Partner a non-exclusive, non-transferable trial license to store, load, install, and use the Product or its components for its internal evaluation business purposes for a period of up to thirty (30) calendar days and limited by one (1) Customer's brand/trademark from the Effective date with no charge. Kaspersky may upon mutual written agreement (including via email), extend the Period of this Trial Use License.

Trial Use License is a time-limited and/or functionality-limited license to use the Product in accordance with these Product T&C. Trial use is available for a limited Period, and in format of Demo use, or Pilot project mode. Parameters and limitations, Trial use format is previously agreed by the Parties in writing (including via email), or stated in the Proposal, or in the Order. Usage of Trial Use License indicates Customer's or Partner's acceptance of any such parameters and limitations.

Kaspersky reserves all rights to provide Pilot projects on a royalty-free and/or commercial basis. All conditions of Trial use, including but not limited to terms of subscription, functionality, scope of the extended support of Kaspersky team, etc. are previously agreed by Parties in written including via email.

Demo use can be limited by functionality, provided at the time of Customer's or Partner's access.

- 2.3.** Access to Product. The Product is provided by means of granting access to Kaspersky TIP. Customer credentials and digital certificate or TOTP code for Kaspersky TIP access are delivered via encrypted email communication to the email address specified by Customer. Customer is not allowed to share credentials and/or digital certificates/TOTP code with anyone. Real-time threat notifications will be delivered to Kaspersky TIP. Customer will be able to obtain information from the Kaspersky TIP itself or using restful API.

Kaspersky may immediately suspend/terminate access if: (i) payment overdue > ten (10) days; (ii) breach of license restrictions; (iii) excessive API abuse; or (iv) regulatory/sanctions issues. No refunds for partial periods are then available. Pre-paid fees remain due.

- 2.4.** Compensation. The License fee and payment procedure and details shall be stipulated in the Order and/or in the Direct agreement. Obligations of Kaspersky hereunder shall be subject to and conditioned upon the confirmation from Customer or Partner that the payment terms for the Product have been fully accepted and acknowledged by Customer or Partner and Kaspersky received a valid Order in respect of these Product. Customer or Partner hereby agrees to pay License fee in due order. Unless otherwise agreed in writing, all amounts are exclusive of value added tax, sales tax, or other applicable taxes, which shall be payable by Customer or Partner in addition to license fees. In the event of delayed payment beyond ten (10) Business days after the due date, Kaspersky may suspend the provision of Product until full payment is received, without prejudice to any other rights or remedies available. Kaspersky may charge interest on overdue amounts at a rate of fifteen (15) % per annum or the maximum rate permitted by applicable law, calculated from the due date until payment is received.

- 2.5.** Term. The Product T&C shall commence on (i) the Effective Date, (ii) the date of Customer or Partner acceptance of these Product T&C, by clicking the appropriate buttons if required by Kaspersky. The Product T&C becomes not applicable as soon as the Period is expired unless the initial Period is extended or renewed by a new Order, or otherwise agreed by Parties in written, including via email.

- 2.6.** Cooperation. Customer or Partner shall provide the access to its information and property as may be reasonably required in order to permit Kaspersky to perform its obligations hereunder. Kaspersky will not be liable if information or materials provided to Kaspersky by the Customer or Partner are unavailable, inaccurate, and/or inadequate for the Product delivery. Kaspersky will use commercially reasonable efforts to work with the Customer or Partner to correct or clarify any inaccuracies in the Customer's or Partner's information or materials.

- 2.7.** Technical Support. During the term of license purchased Kaspersky provides Customer or Partner with Technical Support, which includes resolution of Customer or Partner problems related to the Product use and being utilized properly according to its intended use and in compliance with the documentation and technical specifications, and these Product T&C.

Kaspersky Technical Support/Customer Service specialists make every commercially reasonable effort to provide quality support within reasonable time, depending on the nature of the request.

Obligations to respond within a fixed period of time can only be offered as part of [paid services](#).

Customer can ask Kaspersky via [the contact page](#) or use a dedicated "Contact support" button in Kaspersky TIP, if technical support is needed.

2.7.1. Standard Support does not include the following:

- Development of new Product functionality at the request of a User;
- Performance improvement and configuring of User's devices;

- Onsite Support and Remote Support sessions (can be bought as an additional service within Kaspersky Professional Services);
- Assisting a User on the phone or via web chat while collecting data for analysis and/or application of recommendations;
- Consultations regarding third-party applications and/or operating systems;
- Use of third-party patches for operating systems and applications to fix vulnerabilities
- Integration of Kaspersky Software with third-party software (can be bought as an additional service within Kaspersky Professional Services);
- Configuring and checking the Software performance by Technical Support/Customer Service specialists and advice on configuring network security (can be bought as an additional service within Kaspersky Professional Services);
- Software training;
- Demonstration, deployment, and configuration of Software (can be bought as an additional service within Kaspersky Professional Services);
- Analysis and provision of an official opinion on causes of a technical error;
- Analysis and investigation of the causes of incidents resulting from malware infection (can be bought as an additional service within Kaspersky Incident Response).

2.7.2. Kaspersky does not provide Support in the following cases:

- Hardware and/or platform-specific software does not meet the minimum system requirements for the Product;
- Product version is no longer supported (support renewal can be bought upon request).

2.7.3. Kaspersky does not guarantee successful installation, stable Product operation, and resolution of problems in the following cases:

- Software interruptions are caused by hardware issues.
- Software interruptions are caused by incompatible versions of platform-specific software.
- The User is unable or refuses to provide Kaspersky Technical Support/Customer Service specialists with the information that is required to reproduce, analyze, and fix the specific problem.
- The problem arose due to incorrect use or disregard of instructions provided by Kaspersky Technical Support/Customer Service specialists or Kaspersky documentation.

2.7.4. Kaspersky provides Support under the following conditions:

- All commercial and trial versions are supported regardless of the license status.
- A valid license is required for support of all commercial versions of Product.

Some services that are not included in Standard Support may be offered as part of [paid services](#).

2.7.5. Kaspersky guarantees the provision of Technical Support/Customer Service for the Product in accordance with these Product T&C.

2.7.6. Kaspersky Technical Support/Customer Service specialists may ask the User to execute additional Kaspersky utilities (software tools) if this is deemed necessary for handling a request.

2.7.7. After processing a request and on a periodic basis, Kaspersky has the right to ask the User for feedback on the quality of service.

2.7.8. When communicating with Technical Support/Customer Service specialists, the User must provide Kaspersky with timely responses, information about the purchased License, and any information reasonably necessary to properly process the request.

2.7.9. Kaspersky may terminate Support if Customer: (i) exceeds Asset limits; (ii) shares credentials; or (iii) uses Product improperly

3. MISCELLANEOUS

- 3.1.** Customer is aware that: (i) Kaspersky does not guarantee, that it will detect and mitigate all brand abuse, impersonations, and all other online threats during the Product use, (ii) the quality of the Brand monitoring depends on assets, provided by Customer to Kaspersky, and (iii) Kaspersky does not provide any legal or reputational verdicts.
- 3.2.** Kaspersky reserves the right at any time to improve the Product and/or its components (including without limitation content, format, delivery, update details, number of records, sources of intelligence and internal manuals). Content of the Product, its features and/or its format is subject to change and not all their features are available at all times.
- 3.3.** If Customer or Partner violates any of its obligations hereof or License limitations stipulated in these Product T&C or other legally binding document concluded between Kaspersky and Customer or Partner related to the Product, Kaspersky may stop or suspend its delivery. No refund is due in such event.
- 3.4.** Customer may provide Kaspersky with Mobile app link and Social Network account link, domains, brands or keywords relevant to Customer's organization as a part of the scope of analysis. This information can be provided on the relevant tab of Kaspersky Threat Intelligence Portal. Kaspersky reserves the right to evaluate the provided resources specified by Customer as inappropriate for analysis within the Product.
- 3.5.** Kaspersky does not covenant, guarantee or warrant that Customer will not be attacked during the Product use, as a goal of the Product is to analyze threats specific to the Customer, and notify the Customer about threat intelligence finding.
- 3.6.** Customer may not remove or alter any copyright notices or other proprietary notices of the Product, related documentation or materials. All rights not expressly granted herein are reserved by Kaspersky and its licensors.
- 3.7.** Kaspersky reserves the right at any time to modify (by posting on its website or via email to the contact provided by Customer/Partner) these Product T&C and to impose new or additional terms or conditions on the Product use. Such modifications will be effective immediately when incorporated into the Product T&C. Continued use of the Product by Customer or Partner will be deemed acceptance thereof.
- 3.8.** Neither party shall assign or transfer its rights nor delegate its obligations under these Product T&C without the prior written consent of the other party, save that Kaspersky may assign these Product T&C to an affiliate or in the connection with a merger or acquisition without restriction.
- 3.9.** Unless otherwise is stated in the Agreement, these Product T&C are governed by the material laws of Germany. Any disputes arising out of or in connection with these Product T&C shall be subject to the exclusive jurisdiction of the courts of country where Kaspersky entity rendering the services is located.
- 3.10.** To the extent Kaspersky processes any personal data on behalf of the Customer/Partner, such processing shall be in accordance with the Data Processing Addendum, available upon request or as set forth in the Agreement.

- 3.11.** Unless otherwise is stated in the Agreement, and to the maximum extent permitted by applicable law, in no event shall Kaspersky, its affiliates, or licensors be liable for any indirect, incidental, special, consequential or punitive damages, or for any loss of profits or revenues, whether incurred directly or indirectly, or any loss of data, use, goodwill, or other intangible losses, resulting from Customer's use of or inability to use the Product, even if Kaspersky has been advised of the possibility of such damages. The aggregate liability of Kaspersky under these Product T&C shall not exceed the fees paid or payable by Customer for the Product in the twelve (12) months preceding the event giving rise to the liability.
- 3.12.** No delay or omission by either party in exercising any right under these Product T&C shall operate as a waiver of that or any other right. A waiver or consent given by a party on any one occasion shall be effective only in that instance and shall not be construed as a bar or waiver of any right on any other occasion. In the event that any provision of the Product T&C shall be invalid, illegal or otherwise unenforceable, the validity, legality and enforceability of the remaining provisions shall in no way be affected or impaired. This Agreement may also be amended or modified by a written instrument executed by both the Customer or Partner and Kaspersky or by Kaspersky only as stipulated in clause 3.7. of these Product T&C.

THESE PRODUCT T&C SHALL BE BINDING UPON, AND INURE TO THE BENEFIT OF, BOTH PARTIES AND THEIR RESPECTIVE SUCCESSORS AND ASSIGNS.