

KASPERSKY THREAT LOOKUP

PRODUCT TERMS AND CONDITIONS

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

These Product T&Cs are legally binding and govern Customer and Partner use of Kaspersky Threat Lookup ('the Product'). Accordingly, Kaspersky advises reading 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), the Customer or Partner accepts and agrees to be bound by these Product T&Cs 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&Cs and comply with them.

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

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

In the event of any conflict between the provisions of these Product T&Cs 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 T&Cs supplement the separate Agreement and take precedence over any Customer/Partner purchase order or similar document.

1. DESCRIPTION

Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky about cyberthreats and their relationships, combined into a single, powerful web solution. The goal is to provide Customer security teams with as much data as possible, preventing cyberattacks before they affect the Customer organization. The platform retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat actors, CVEs, WHOIS/DNS data, etc. The result is global visibility into new and emerging threats, helping to secure the Customer's organization and boosting incident response.

Key Features

Trusted Intelligence: A key attribute of the Product is the reliability of Kaspersky threat intelligence data, enriched with actionable context. Kaspersky products lead the field in anti-malware tests, demonstrating the unequalled quality of our threat intelligence by delivering the highest detection rates, with near-zero false positives.

High levels of real-time coverage: Threat intelligence is automatically generated in real time, based on global findings, providing wide coverage and high accuracy.

Threat hunting: Be proactive in preventing, detecting and responding to attacks, to minimize their impact and frequency. Hunt and eliminate attacks as early as possible. The earlier the Customer can discover a threat - the less damage is caused, the quicker mitigation takes place and the sooner network operations returns to normal.

Rich data: Threat intelligence delivered by Kaspersky Threat Lookup covers a wide range of different data types, including hashes, URLs, IPs, WHOIS, pDNS, GeoIP, file attributes, statistical and behavior data, download chains, timestamps and much more. Empowered with this data, the Customer can survey the diverse and evolving threat landscape they're facing.

Continuous availability: Threat intelligence is generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability and consistent performance.

Continuous review by security experts: Hundreds of experts, including security analysts from across the globe, leading security experts from the Kaspersky GReAT team and pioneering R&D teams contribute to generating valuable real-world threat intelligence.

Wide range of export formats: Export IOCs (Indicators of Compromise) or actionable context into widely used and more specific machine-readable sharing formats, such as STIX, OpenIOC or CSV to derive the full benefits of threat intelligence, automate operational workflow, or integrate into security controls such as SIEMs.

Easy-to-use web interface or RESTful API: Use the Product in manual mode through a web interface (via a web browser) or access it via a simple RESTful API.

Benefits

- ▶ **Improve and accelerate incident response and forensic capabilities** by equipping the Customer's security/SOC team with meaningful information about threats, and global insights into what lies behind targeted attacks. Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats, minimizing incident response times and disrupting the kill chain before critical systems and data are compromised.
- **Conduct deep searches into threat indicators** such as IP addresses, URLs, domains or file hashes, with highly-validated threat context that allows the Customer to prioritize attacks, improve staffing and resource allocation decisions, and focus on mitigating the threats that pose the most risk to the Customer's business.
- **Mitigate targeted attacks.** Enhance the Customer's security infrastructure with tactical threat intelligence by adapting defensive strategies to counter the specific threats the Customer's organization faces.

With access to **Kaspersky Threat Lookup**, the Customer can:

- ✓ Look up threat indicators via a web-based interface or via the RESTful API.
- ✓ Understand why an object should be treated as malicious.
- ✓ Check whether the discovered object is widespread or unique.
- ✓ Examine advanced details including certificates, commonly used names, file paths, or related URLs to discover new suspicious objects.

The Customer can look up information about:

- ✓ IP addresses
- ✓ Domains
- ✓ Hashes
- ✓ URLs
- ✓ Actor names
- ✓ Software name
- ✓ CVEs
- ✓ Keywords (text search in Threat Intelligence Reports and Dark/Surface web)

The Product provides the following general information about hashes:

- **Status** – Shows whether the requested hash can be classified as malicious.
- **Hits** – Number of hits (popularity) of the requested hash detected by expert systems.
- **First seen** – Date and time when the requested hash was detected by Kaspersky expert systems for the first time.
- **Last seen** – Date and time when the requested hash was detected by Kaspersky expert systems for the last time.
- **Format** – Format of the object being investigated by hash.

- **Size** – Size of the object being investigated by hash (in bytes).
- **Signed by** – Organization that signed the requested hash.
- **Packed by** – Packer name (if any).
- **MD5** – MD5 hash function of the file requested by hash.
- **SHA-1** – SHA-1 hash function of the file requested by hash.
- **SHA-256** – SHA-256 hash function of the file requested by hash.
- **Category** – Shows whether the file identified by the requested hash is related to an advanced persistent threat (APT) attack.

The Product displays, in separate tables, additional information about the hash that is being investigated. The Customer can export data from these tables as separate archives.

The Product provides the following general information about IP addresses:

- **Status** – Shows whether the requested IP address generates malicious activity.
- **Hits** – Hit number (popularity) of the requested IP address.
- **First seen** – Date and time when the requested IP address appeared in expert systems statistics for the first time.
- **Threat score** – Probability that the requested IP address will appear dangerous (0 to 100).
- **Owner name** – Name of the requested IP address owner.
- **Owner ID** – ID of the requested IP address owner.
- **Created** – Date when the requested IP address was registered.
- **Updated** – Date when information about the requested IP address was last updated.
- **Category** – Category of the requested IP address.
- **Industries** – Industries the requested IP relates to.

The Product provides additional information about the requested IP address displayed in separate tables. The Customer can export data from these tables as separate archives.

The Product provides the following general information about Domains/URLs:

- **Status** – Shows whether the requested domain and web address can be classified as malicious, good, or not categorized.
- **IPv4 count** – Number of known IP addresses related to the requested domain and web address URL.
- **Files count** – Number of known malicious / all files.
- **Created** – Domain creation date.
- **Expires** – Domain expiration date.
- **Domain** – Name of the upper-level domain.
- **Registration organization** – Name of the registration organization.
- **Registrar name** – Name of the domain name registrar.
- **Owner name** – Domain owner name.
- **Category** – Category of the requested domain and web address.
- **Industries** – Industries the requested domain and web address relates to.

OSINT IoCs

In addition to lookup results, the Product provides open-source intelligence (OSINT) for the requested IoCs, threat actor names, software used by adversaries and CVE. This allows the Customer to find more information on IoCs, for example, in posts in which an IoC is mentioned.

An additional license is required to accessing the API in order to obtain AI-generated data in the OSINT section of Kaspersky Threat Lookup from third-party XDR and/or SIEM and/or SOAR type software in the Russian Federation, Republic of Belarus, and Kazakhstan.

The Product displays a list of posts in which the requested keyword is mentioned on the OSINT IoCs page. AI summarization may also be provided if enough data is available in OSINT sources.

The search results for a requested hash include results for all of its types, such as MD5, SHA-1 and SHA-256. For example, if the Customer searches for MD5 hash, posts on MD5, SHA-1 and SHA-256 hashes of the file are also shown.

Dark Web and Surface Web Section

The Product allows the running of a full-text search against a limited set of Dark Web or other hidden publications and against a limited set of publications in various social media.

For the Dark Web posts and other hidden publications, the Product supports [simple Elasticsearch queries](#).

Search results are displayed on the Dark web page and the Surface Web page of the Product.

By default, the Product searches forums, messengers, ransomware blogs, news, and pastes categories.

Threat Intelligence Sources:

Threat intelligence is aggregated from a fusion of heterogeneous and highly reliable sources, including the Kaspersky Security Network (KSN) and Kaspersky's own web crawlers, Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), spam traps, research teams, partners and other historical data about malicious objects collected by Kaspersky over almost three (3) decades. Then, in real time, all aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, Kaspersky expert systems (sandboxes, heuristics engines, similarity tools, behavior profiling etc.), analyst validation and allowlisting verification.

Saved Searches

The Product allows the creation of search requests which are repeated periodically, so the Customer can track and analyze changes to specific objects. Search requests can be created for any of the following objects:

- **Hash**
- **IP address**
- **Domain name**
- **Web address**
- **Text input:** specific word or phrase for the full-text search

The search is conducted through one or several described services (Lookup/Dark Web). The Customer can also specify one or several sections/categories for the search. The search request will be repeated every twenty-four (24) hours and if any changes or new information fall under the specified rule, it will be reflected in the Kaspersky Threat Intelligence Portal (TIP).

Research Graph

The Kaspersky TIP research graph is an analytical tool for visualizing relationships between various types of objects (files, web addresses, domains, IP addresses, actors, or reports) analyzed and detected during the research.

The information is presented in graphs as nodes (for objects) and relationships that show connections between the nodes. Each object in the research graph can be represented by only one node: object, section, or group.

When the research graph represents analysis results for the object submitted to the Product, this object is shown as a node in the research graph. This includes group nodes for files transferred or dropped during file execution in the Kaspersky sandbox, groups of web addresses and domains accessed during execution.

Research graphs can be created by the Customer, or existing graphs edited for the analyzed objects. The Customer's personal limit for the number of graphs created is displayed on the Research Graph page. If the limit is exceeded, the Customer needs to delete unnecessary research graphs.

Research graph data is updated only based on the results of look ups initiated by the Customer editing the research graph.

The Research graph allows the adding of the following objects:

- **Hash**
- **IP address**
- **Domain name**
- **Web address**
- **Actor**
- **Report**
- **Custom object**

On the graph, the Customer can check detailed information about the node (object).

Product Options

The Product is available in the following options:

- Standalone Kaspersky Threat Lookup with access to full functionality.
- Kaspersky Threat Lookup Lite, created for scenarios where automated lookups are initiated from other products/services. This option provides basic information about a URL, Domain, IP, or Hash via a simple RESTful API.
- As a part of other products/services.
- Kaspersky Threat Lookup, limited to fifty (50) searches per day, is available for the customers of Kaspersky Digital Footprint Intelligence.

The type and price of the Product is indicated in the Proposal, and/or in the Kaspersky price list in effect at the time when the order is placed, which the Customer or Partner declares that they know and accept. The current price list shall supersede all previous price lists. The Product may be purchased for different Subscription Periods.

The License is limited by the fixed number of searches permitted per day. The number of searches varies from 100 to 10,000 searches per day.

Kaspersky will provide the Product option(s) in accordance with the Order, Certificate and these Product T&Cs.

Kaspersky Threat Lookup & Analysis Bundles

The Product is included in the following Kaspersky Threat Lookup & Analysis Bundles, available for purchase: **Basic, Essential and Advanced.**

Kaspersky Threat Lookup & Analysis Bundles Composition:

<i>PRODUCTS AND SCOPE</i>	<i>BASIC</i>	<i>ESSENTIAL</i>	<i>ADVANCED</i>
Kaspersky Threat Lookup — Access to database of threat indicators — Research graph — WHOIS hunting rules — 10 saved searches	1, 000 requests	2, 000 requests	3, 000 requests
Threat Analysis — Cloud Sandbox — Cloud Threat Attribution Engine — Similarity	100 requests for each technology	150 requests for each technology	200 requests for each technology
	per 1 year		

Kaspersky Threat Lookup & Dark Web Search bundle

Kaspersky Threat Lookup & Dark Web Search MSSP is limited by the number of searches per day. This bundle is available for a one (1) year Subscription Period.

Kaspersky Threat Intelligence Bundles

The Product is included in the following Kaspersky Threat Intelligence Bundles, available for purchase.

Threat Intelligence Bundles	Kaspersky Threat Lookup	Details of the functional scope
BASIC	1,000 requests per one (1) year	— Access to database of threat indicators
ESSENTIAL	2,000 requests per one (1) year	— Research graph
ADVANCED	3,000 requests per one (1) year	— WHOIS Hinting Rules
EXPERT	10,000 requests per one (1) year	— Ten (10) saved searches
MAXIMUM	50,000 requests per one (1) year	

Kaspersky Threat Intelligence Bundles Composition:

PRODUCTS AND SCOPE	BASIC	ESSENTIAL	ADVANCED	EXPERT	MAXIMUM
Kaspersky Threat Lookup — Access to database of threat indicators — Research graph — WHOIS hunting rules — 10 saved searches	1 000 requests	2 000 requests	3 000 requests	10 000 requests	50 000 requests
	per 1 year				
Threat Infrastructure Tracking	-	-	Country level	Full access	Full access
Digital Footprint Intelligence — External perimeter analysis — Dark Web monitoring — Discovery of data leaks — Threat detection	-	+	+	+	+
APT Reporting — Reports — Actor profiles — IoC and YARA	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Crimeware Reporting — Reports — Actor profiles — IoC and YARA	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Threat Analysis — Cloud Sandbox — Cloud Threat Attribution Engine — Similarity	100 requests	150 requests	200 requests	1 000 requests	3 000 requests
	per 1 year for each technology				

MSSP Bundle Composition

There are different Kaspersky Threat Intelligence Bundles created especially for MP partners.

Licenses are available for one (1) year or one (1) month Subscription Periods.

Kaspersky Threat Lookup & Dark Web Search MSSP

PRODUCT NAME	LICENSE MODEL	MIN INITIAL PURCHASE	SUBSCRIPTION PER YEAR	SUBSCRIPTION PER MONTH
Kaspersky Threat Lookup & Dark Web Search MSSP	By number of searches per month	500	+	+

Kaspersky Threat Intelligence Bundles

PRODUCTS AND SCOPE	BASIC MSSP	ESSENTIAL MSSP	ADVANCED MSSP	EXPERT MSSP	MAXIMUM MSSP
Kaspersky Threat Lookup — Access to database of threat indicators — Research graph — WHOIS Hinting Rules — 10 saved searches	1 000 requests	2 000 requests	3 000 requests	10 000 requests	50 000 requests
	per 1 year				
Threat Infrastructure Tracking	-	-	Country level	Full access	Full access
Digital Footprint Intelligence — External perimeter analysis — Dark web monitoring — Discovery of data leaks — Threat detection	-	5 End-Users	5 End-Users	5 End-Users	5 End-Users
APT Reporting — Reports — Actor profiles — IoC and YARA	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Crimeware Reporting — Reports — Actor profiles — IoC and YARA	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Dark Web search — Forums — IT Forums — Messengers — Ransomware blogs — News	-	+	+	+	+
Threat Analysis — Cloud Sandbox — Cloud Threat Attribution Engine — Similarity	100 requests	150 requests	200 requests	1000 requests	3000 requests
	per 1 year				

Kaspersky reserves the right to change the composition of the Kaspersky Bundles and/or its components at any time in order to improve its value to the Customer or Partner. The actual composition of the Bundles is set out in the Proposal and/or in the Kaspersky's price list in effect at the time of placing the Order, or by request prior to placing the Order.

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

2. DELIVERY

- 2.1.** License. Kaspersky grants the Customer or Partner a non-exclusive, non-transferable limited license to access the Kaspersky threat intelligence database and software for a defined period, allowing the searching of the required information relating to threats, up to and including the

maximum number of searches permitted per day, strictly in accordance with documentation provided by Kaspersky, and solely for the Customer's or Partner's internal business purposes. No right to extract, republish, or commercially exploit Threat Intelligence data is granted.

2.2. MP License. Kaspersky grants the MP Partner a non-exclusive, non-refundable, non-transferable, limited, revocable license for a defined period in order to:

- where applicable, install, integrate, execute, reproduce, display, copy for archival purposes, transmit internally, and use the Product and its components on the MP Partner's server(s) and/or computer system(s) for the purpose of creating, maintaining, providing and supporting the MP Partner's products and services.
- provide the MP Partner's End User(s) with access to, and the right to use, the Product solely as part of the MP Partner's products and services as managed by the MP Partner in accordance with the Order, the conditions of Trial use, and the Product T&Cs.
- permit the End User(s) to access and use the Product solely as part of the MP Partner's products and services, subject to the terms of the MP End-User Agreement. 'MP End-User Agreement' means an agreement executed between the MP Partner and the MP End User for the provision of the MP Partner's products and services, which is no less restrictive and no less protective of Kaspersky's rights than these Product T&Cs.

2.3. Trial Use License. Kaspersky grants the Customer or Partner a non-exclusive, non-transferable trial license to store, load, install, and use the Product or its components for internal business evaluation purposes for a period of up to thirty (30) calendar days from the Effective Date, at no charge. Kaspersky may, upon mutual written agreement (including via email), extend the Period of this Trial Use License.

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

Kaspersky reserves the right to provide Pilot projects on a royalty-free and/or commercial basis. All conditions of Trial use, including without limitation, subscription terms, functionality, and the scope of any extended support provided by the Kaspersky team, are agreed in advance by both Parties in writing (including via email).

Demo use can be limited in functionality, as specified at the time when the Customer or Partner is granted access.

2.4. Access to the Product. The Product is provided by means of granting access to Kaspersky TIP via UI or API. Customer credentials and the digital certificate for access to the Portal are delivered via encrypted email communication to the email address specified by the Customer.

2.5. Compensation. The License fee, payment procedure and details shall be stipulated in the applicable Order and/or Direct Agreement. Kaspersky's obligations hereunder shall be subject to and conditional upon the Customer's or Partner's confirmation that the payment terms for the Product have been fully accepted and acknowledged, and that Kaspersky has received a valid Order in respect of the Product. The Customer or Partner hereby agrees to pay the applicable License fee in accordance with the payment terms of the 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 the Customer or Partner in addition to the license fees. In the event of payment delay exceeding ten (10) Business days after the due date, Kaspersky may suspend provision of Product until full payment is received, without prejudice to any other rights or remedies available to

Kaspersky. Kaspersky may charge interest on overdue amounts at a rate of fifteen percent (15%) per annum, or the maximum rate permitted by any applicable law, calculated from the due date until payment is received in full.

- 2.6.** Term. The Product T&Cs shall commence on (i) the Effective Date, or (ii) the date the Customer or Partner accepts these Product T&Cs, by clicking on the appropriate buttons if required by Kaspersky. These Product T&Cs shall cease to apply upon expiration of the Period, unless the initial Period is extended or renewed by a new Order, or otherwise agreed by Parties in writing, including via email.
- 2.7.** Cooperation. The Customer or Partner shall provide access to such 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 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.
- 2.8.** Technical Support. During the term of the license, will Kaspersky provide the Customer or Partner with Technical Support for the purchased Product, which includes assistance with resolving issues related to the use of the Product, provided that the Product is used in accordance with its intended purpose, Product documentation and technical specifications, and these Product T&Cs.

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

Any obligation to respond within a fixed period of time is only offered as part of [paid services](#).

The Customer may contact Kaspersky via [the contact page](#) or by using the dedicated "Contact support" button in Kaspersky TIP, if technical support is needed.

2.8.1. 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 purchased 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 the 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 purchased as an additional service within Kaspersky Professional Services).
- Configuring and checking of Software performance by Technical Support/Customer Service specialists and advice on configuring network security (can be purchased as an additional service within Kaspersky Professional Services).
- Software training.
- Demonstration, deployment, and configuration of Software (can be purchased as an additional service within Kaspersky Professional Services).
- Analysis and provision of an official verdict on the causes of a technical error.
- Analysis and investigation of the causes of incidents resulting from malware infection (can be purchased as an additional service within Kaspersky Incident Response).

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

- If hardware and/or platform-specific software does not meet the minimum system requirements for the Product.

- If the Product version is no longer supported (support renewal can be purchased on request).

2.8.3. Kaspersky does not guarantee successful installation, stable Product operation, or resolution of problems in cases where:

- Software interruption is caused by hardware issues.
- Software interruption is 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 required to reproduce, analyze, and fix a specific problem.
- A problem arises due to the incorrect use or disregard of instructions provided by Kaspersky Technical Support/Customer Service specialists or Kaspersky documentation.

2.8.4. Kaspersky provides Support under the following conditions:

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

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

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

2.8.6. 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.

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

2.8.8. 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.

3. MISCELLANEOUS

- 3.1.** MP Partners shall guarantee that they are authorized by their End User(s) and have all necessary Agreements with their End User(s) in accordance with any applicable law, and all necessary rights and permissions to use the Product on the End-User(s) behalf.
- 3.2.** Kaspersky reserves the right at any time to improve the Product and/or its components (including without limitation its 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 features are available at all times.
- 3.3.** If the Customer or Partner violates any of its obligations or License limitations stipulated in these Product T&Cs, or any other legally binding document concluded between Kaspersky and the Customer or Partner related to the Product, Kaspersky may stop or suspend its delivery. No refund is due in this case.
- 3.4.** No sample uploaded by the Customer may be disclosed, transmitted, or otherwise made available to any third party, and all such samples are stored solely within Kaspersky's controlled infrastructure.
- 3.5.** Kaspersky does not covenant, guarantee or warrant that the Customer will not be subjected to cyberattacks during use of the Product. The purpose of the Product is to analyze threats specific

to the Customer, to notify the Customer of relevant threat intelligence findings and to provide recommendations for further remediation.

- 3.6.** The Customer may not remove or alter any copyright notices or other proprietary notices relating to the Product or any 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 the Customer or Partner) these Product T&Cs and to impose new or additional terms or conditions on Product use. Such modifications will be effective immediately they are incorporated into the Product T&Cs. Continued use of the Product by the Customer or Partner will be deemed acceptance thereof.
- 3.8.** Neither party may assign or transfer its rights or delegate its obligations under these Product T&Cs without the prior written consent of the other party, except that Kaspersky may assign these Product T&Cs without restriction to an affiliate or in the context of a merger or acquisition.
- 3.9.** Unless otherwise is stated in the Agreement, these Product T&Cs are governed by the material laws of Germany. Any disputes arising out of or in connection with these Product T&Cs shall be subject to the exclusive jurisdiction of the courts of the country in which the Kaspersky entity providing the services is located.
- 3.10.** To the extent that Kaspersky processes any personal data on behalf of the Customer or Partner, such processing shall be carried out in accordance with the Data Processing Addendum, available on 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 for any loss of data, use, goodwill, or other intangible losses, arising out of or relating to the Customer's or Partner use of or inability to use the Product, even if Kaspersky has been advised of the possibility of such damages. Kaspersky's aggregate liability under these Product T&Cs shall not exceed the fees paid or payable by the Customer (or Partner as the case may be) 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&Cs 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. If any provision of the Product T&Cs 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&Cs.

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