File Inspection Platform Terms of Service

Trinity Cyber

Trinity Cyber Terms of Service Agreement

The Trinity Cyber File Inspection Platform is offered as a federated Application Programming Interface (API) service. Trinity Cyber's file inspection service, file parser application, program modules, test suites and tools are collectively referred to as the Service or API's, interchangeably. By accessing or using the Service, or any associated software, you agree and consent to these Terms of Service including terms herein that limit our liability or affect your legal rights, any referenced and incorporated guidelines and policies, terms within the accompanying API documentation, and any additional terms specific to your particular use of the Service that become part of your agreement with Trinity Cyber (collectively, the "Terms"). If you are using the Service on behalf of a business, you represent to us that you have authority to bind that business or entity to these Terms, and that the business accepts these Terms. You agree to comply with the Terms and that the Terms control your relationship with us. So PLEASE READ ALL THE TERMS CAREFULLY BEFORE USING OR ACCESSING TRINITY CYBER SOLUTIONS, SOFTWARE, OR SERVICES.

Under the Terms, "Trinity Cyber" means Trinity Cyber, Inc., with offices at 16701 Melford Blvd., Suite 300, Bowie, Maryland, 20715, United States. We may refer to "Trinity Cyber" as "we", "our", or "us" in the Terms.

The following terms govern your use of the Service except to the extent a particular program (a) is the subject of a separate written agreement with Trinity Cyber or (b) includes a separate "click-on" license agreement as part of the installation and/or download or upload process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, if any, and (3) this Terms of Service agreement.

Section 1: Definitions

a. File

A computer file is an object on a computer that stores information, settings, or commands used with a computer program, referred to generally herein as file data. There are multiple categories of files including application files, data files, and system files. There are multiple types of files within these categories including document files, files containing executable programs or processes, and script files. While Trinity Cyber parses and fully inspects many common categories and types of files, and reserves the right to deploy new file parsers at its discretion, it makes no guarantee that it can parse or fully inspect all categories and types of files.

b. Metadata

Metadata means a set of data that describes and gives information about the file data submitted by Customer. Specifically, Trinity Cyber metadata will include, at a minimum, a true or false judgement on whether a file contains malicious or suspicious content that might do harm to any recipient's computer, network, or digitized data or that might allow or facilitate unauthorized access to the same. Whenever possible and applicable, metadata provided by Trinity Cyber will include a list of threat intelligence information on the name of the malware believed to be in the file, the malware classification, exploit name, exploit type, the Common Vulnerabilities and Exposures (CVE) targeted, hacking techniques being attempted, and the stage of the Unified Kill Chain in which this information is most commonly categorized.

Section 2: Service Description

Trinity Cyber operates an advanced parsing, scanning, inspection and sanitization technology (or "Trinity Security Engine") capable of rapidly (a) inspecting computer files for the presence of malicious or suspicious content and reporting the findings of that inspection to a Customer, and (b) inspecting computer files for the presence of malicious or suspicious content, reporting the findings to a Customer, and returning those files deemed malicious or suspicious in an altered form meant to render such files benign. The former is sold as a "Threat Detection" service and the latter as a "File Cleaning" service. Trinity Cyber also sells access to its File Parser application and Client Portal. Trinity Cyber reports to Customer relevant information, referred to as metadata, concerning its detection of malicious or suspicious content and, if providing File Cleaning service, an explanation of how and why a file was altered.

The Customer receives metadata from Trinity Cyber in the Threat Detection service setting. The Customer receives metadata plus encoded file content from Trinity Cyber in the File Cleaning service setting.

Trinity Cyber agrees to provide Customer with access to the Trinity Cyber Application Programming Interface (or "API") and valid credentials in the form of an API key, or any other open authentication scheme deemed appropriate. Trinity Cyber agrees to make all reasonable efforts to permit and maintain uninterrupted Customer access to the Service.

Trinity Cyber will (1) operate, maintain, and regularly update at its discretion the Trinity Security Engine, (2) apply its parsers and formulas to files submitted by paying Customers; (3) provide metadata to the Customer pertaining to each file, or metadata plus altered file content when providing the File Cleaning service; and (4) maintain at all times the ability to perform the Service with minimal latency and in keeping with the performance claims and guarantees contained in the Trinity Cyber File Inspection Platform Service Level Agreement (SLA).

a. Threat Detection

Trinity Cyber will receive files from the Customer, scan the file data using its proprietary technology, and provide the Customer metadata pertaining to each file through the Trinity Cyber API. Metadata pertaining to any file is meant to support, inform, or in many cases render a judgement on the security risk posed by the file and to assist the Customer in classifying files as normal, suspicious, or dangerous. Trinity Cyber cannot guarantee its judgement or results will always be correct.

b. File Cleaning

Customer agrees that Trinity Cyber may for the purpose of security alter and return all or part of any file submitted to it for cleaning, and that Trinity Cyber will determine in its sole discretion which files to alter based on its judgement that a file contains malicious or suspicious content and that the file can be altered in a manner that supports the return of a safe file. Trinity Cyber agrees to work in good faith to conform the metadata from Trinity Cyber's API to the Customer's technical and business processes. The Customer agrees that it will in good faith develop the technical means to receive Trinity Cyber's metadata and altered file content.

c. Client Portal and File Parser Access

Depending on the service for which the Customer has agreed to pay, Trinity Cyber will deliver reporting of actions taken to alter files in the File Cleaning setting through a Client Portal or grant access to the Trinity Cyber File Parser application. ***Optional Customization of API Data.*** Trinity Cyber will whenever possible customize the metadata within its application programming interface (API) to meet the needs of Customer's software intermediaries. Although included in the Solution Fees, Trinity Cyber makes no guarantees on the completion time of such customization other than those set forth in the SLA. Trinity Cyber will make every reasonable effort to coordinate data additions or modifications so as not to effect existing integrations, and may reject modifications if they pose risk to other customers of its File Submission service.

d. Support Services

Trinity Cyber shall provide support services 24 hours a day, seven days a week ("Support Services"). Trinity Cyber will provide Support Services to the Customer, to include operating a 24/7 Operations Center. The Operations Center will be available to Customer at all times. Bulk user Customers may request Trinity Cyber temporarily bypass itself at any time for any reason as an operational failsafe. This shall not affect pricing or billing requirements. Trinity Cyber Support Services are intended as a source of information and insight into the Solution and any threats. Support Services are part of the Solution and included in the Solution price.

Section 3: Account and Registration

a. Accepting the Terms

You may not use the API's and may not accept the Terms if (a) you are not of legal age to form a binding contract with Trinity Cyber, or (b) you are a person barred from using or receiving the API's under the applicable laws of the United States or other countries including the country in which you are resident or from which you use the API's.

b. Entity Level Acceptance

If you are using the API's on behalf of an entity, you represent and warrant that you have authority to bind that entity to the Terms and by accepting the Terms, you are doing so on behalf of that entity (and all references to "you" in the Terms refer to that entity).

c. Registration

In order to access certain API's you may be required to provide certain information (such as identification or contact details) as part of the registration process for the API's, or as part of your continued use of the API's. Any registration information you give to Trinity Cyber will always be accurate and up to date and you'll inform us promptly of any updates.

d. Subsidiaries and Affiliates

Trinity Cyber has subsidiaries and affiliated legal entities. These companies may provide the API's to you on behalf of Trinity Cyber and the Terms will also govern your relationship with these companies.

Section 4: Using Our API's

a. Your End Users

You will require your end users to comply with (and not knowingly enable them to violate) applicable law, regulation, and the Terms.

b. Compliance with Law, Third Party Rights, and Other Trinity Cyber Terms of Service

You will comply with all applicable law, regulation, and third-party rights (including without limitation laws regarding the import or export of data or software, privacy, and local laws). You will not use the API's to encourage or promote illegal activity or violation of third-party rights. You will not violate any other terms of service with Trinity Cyber (or its affiliates).

c. Permitted Access

You will only access (or attempt to access) an API by the means described in the documentation of that API. If Trinity Cyber assigns you developer credentials (e.g. client IDs), you must use them with the applicable API's. You will not misrepresent or mask either your identity or your API Client's identity when using the API's or developer accounts.

d. API Limitations

Trinity Cyber sets and enforces limits on your use of the API's (e.g. limiting the number of files you may submit or the number of users you may serve), in our sole discretion and in accordance with the amount of service for which you have paid. You agree to, and will not attempt to circumvent, such limitations documented with each API. If you would like to use any API beyond these limits, you must obtain Trinity Cyber's express consent (and Trinity Cyber may decline such request or condition acceptance on your agreement to additional terms and/or charges for that use). To seek such approval, contact the relevant Trinity Cyber API team for information.

e. Communication with Trinity Cyber

We may send you certain communications in connection with your use of the API's. Please review the applicable API documentation for information about such communication.

f. Feedback

If you provide feedback or suggestions about our API's, then we (and those we allow) may use such information without obligation to you.

g. Non-Exclusivity

The Terms are non-exclusive. You acknowledge that Trinity Cyber may develop products or services that may compete with API Customers or any other products or services.

h. Data Protection

Appropriate technical and organizational measures have been taken by Trinity Cyber to meet the principles of data protection by design and data protection by default. Trinity Cyber processes customer data with technology segregated from the Internet, makes no attempt to differentiate incidental personal data, does not separately process personal data, and uses state of the art technology and controls to make sure that a Customer that might be a regulated controller or processors of personal data may submit its files to the Service in a manner that satisfies its data protection obligations.

Section 5: Your API Clients

a. API Clients and Monitoring

YOU AGREE THAT TRINITY CYBER MAY MONITOR USE OF THE APIS TO ENSURE QUALITY, IMPROVE TRINITY CYBER PRODUCTS AND SERVICES, AND VERIFY YOUR COMPLIANCE WITH THE TERMS. This monitoring may include Trinity Cyber accessing and using your API Client, for example to identify security issues that could affect Trinity Cyber or its users. You will not interfere with this monitoring. Trinity Cyber may use any technical means to overcome such interference. Trinity Cyber may suspend access to the API's by you or your API Client without notice if we reasonably believe that you are in violation of the Terms.

b. Security

You will use commercially reasonable efforts to protect user information collected by your API Client, including personal data, from unauthorized access or use and will promptly report to your users any unauthorized access or use of such information to the extent required by applicable law.

c. Ownership

Trinity Cyber does not acquire ownership in your API Clients, and by using our API's, you do not acquire ownership of any rights in our API's or the content that is accessed through our API's.

d. User Privacy

You will comply with all applicable privacy laws and regulations including those applying to personal data. Trinity Cyber will not share Customer data or API user identity with any third parties. Trinity Cyber will not reveal Customer names to the public without prior written consent of the Customer.

Section 6: Prohibitions and Confidentiality

a. API Prohibitions

When using the API's, you may not (nor may those acting on your behalf):

1. Sublicense an API for use by a third party. Consequently, you will not create an API Client that functions substantially the same as the API's and offer it for use by third parties.
2. Perform an action with the intent of damaging, gaining unauthorized access to, or stealing Trinity Cyber source code or systems
3. Interfere with or disrupt the API's or the servers or networks providing the API's.
4. Reverse engineer or attempt to extract the source code from any API or any related software, except to the extent that this restriction is expressly prohibited by applicable law.
5. Use the API's for any activities where the use or failure of the API's could lead to death, personal injury, or environmental damage (such as the operation of nuclear facilities, air traffic control, or life support systems).
6. Use the API's to process or store any data that is subject to the International Traffic in Arms Regulations maintained by the U.S. Department of State.
7. Remove, obscure, or alter any Trinity Cyber terms of service or any links to or notices of those terms.

Unless otherwise specified in writing by Trinity Cyber, Trinity Cyber does not intend use of the API's to create obligations under the Health Insurance Portability and Accountability Act, as amended ("HIPAA"), and makes no representations that the API's satisfy HIPAA requirements. If you are (or become) a "covered entity" or "business associate" as defined in HIPAA, you will not use the API's for any purpose or in any manner involving transmitting protected health information to Trinity Cyber unless you have received prior written consent to such use from Trinity Cyber.

b. Confidential Matters

1. Developer credentials (such as passwords, keys, and client IDs) are intended to be used by you and identify your API Client. You will keep your credentials confidential and make reasonable efforts to prevent and discourage other API Clients from using your credentials. Developer credentials may not be embedded in open source projects.
2. Our communications to you and our API's may contain Trinity Cyber confidential information. Trinity Cyber confidential information includes any materials, communications, and information that are marked confidential or that would normally be considered confidential under the circumstances. If you receive any such information, then you will not disclose it to any third party without Trinity Cyber's prior written consent. Trinity Cyber confidential information does not include information that you independently developed, that was rightfully given to you by a third party without confidentiality obligation, or that becomes public through no fault of your own. You may disclose Trinity Cyber confidential information when compelled to do so by law if you provide us reasonable prior notice, unless a court orders that we not receive notice.

Section 7: Content

a. Content Accessible through our API's

The content accessible through our API's may be subject to intellectual property rights, and, if so, you may not use it unless you are licensed to do so by the owner of that content or are otherwise permitted by law. Your access to the content provided by the API may be restricted, limited, or filtered in accordance with applicable law, regulation, and policy.

b. Submission of Content

Our Service allows the submission of file content. While Customer retains any ownership rights in the original file material it submits, when a Customer uploads or otherwise submits a file, it gives Trinity Cyber a worldwide, royalty free, irrevocable and transferable license to use, edit, host, store, reproduce, modify, create derivative works of, communicate, publish, publicly display and distribute all malicious content contained in the file. Malicious content shall never include personal data or personally identifiable information or Customer trade secrets or confidential information.

c. Retrieval of content

You may not expose personal data to other users or to third parties without explicit opt-in consent.

d. Prohibitions on Content

Unless expressly permitted by the content owner or by applicable law, you will not, and will not permit your end users or others acting on your behalf to, do the following with content returned from the API's:

1. Scrape, build databases, or otherwise create permanent copies of such content, or keep cached copies longer than you are a customer of the Service;
2. Copy, translate, modify, create a derivative work of, sell, lease, lend, convey, distribute, publicly display, or sublicense to any third party;
3. Misrepresent the source or ownership; or
4. Remove, obscure, or alter any data returned from the Service, any copyright, trademark, or other proprietary rights notices; or falsify or delete any author attributions, legal notices, or other labels of the origin of the data and metadata returned by the Service unless expressly permitted in writing by Trinity Cyber.

Section 8: Brand Features; Attribution

a. Brand Features

"Brand Features" is defined as the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party. Except where expressly stated, the Terms do not grant either party any right, title, or interest in or to the other party's Brand Features. All use by you of Trinity Cyber's Brand Features (including any goodwill associated therewith) will inure to the benefit of Trinity Cyber.

b. Attribution

You agree to display any attribution(s) required by Trinity Cyber as described in the documentation for the API. Trinity Cyber hereby grants to you a nontransferable, nonsublicenseable, nonexclusive license while the Terms are in effect to display Trinity Cyber's Brand Features for the purpose of promoting or advertising that you use the API's. You must only use the Trinity Cyber Brand Features in accordance with the Terms and for the purpose of fulfilling your obligations under this Section. In using Trinity Cyber's Brand Features, you must follow the Trinity Cyber Brand Features Use Guidelines. You understand and agree that Trinity Cyber has the sole discretion to determine whether your attribution(s) and use of Trinity Cyber's Brand Features are in accordance with the above requirements and guidelines.

c. Publicity

You will not make any statement regarding your use of an API which suggests partnership with, sponsorship by, or endorsement by Trinity Cyber without Trinity Cyber's prior written approval.

d. Promotional and Marketing Use

In the course of promoting, marketing, or demonstrating the API's you are using and the associated Trinity Cyber products, Trinity Cyber may use your company name. You grant us all necessary rights for these purposes.

Section 9: Termination

a. Termination

This Agreement is effective until terminated or until the applicable license or subscription term. You may stop using our API's at any time with or without notice. Further, if you want to terminate the Terms, you must provide Trinity Cyber with prior written notice and upon termination, cease your use of the applicable API's. Subscription fees must be paid until the end of the agreed term unless subject to special trial conditions set forth in the quote for the service. In those special trial conditions, written termination requirements set forth in the quote apply. Trinity Cyber reserves the right to terminate the Terms with you or discontinue the API's or any portion or feature or your access thereto for any reason and at any time without liability or other obligation to you other than an appropriate, prorated refund of fees.

b. Your Obligations Post-Termination

Upon any termination of the Terms or discontinuation of your access to an API, you will immediately stop using the API, cease all use of the Trinity Cyber Brand Features, and delete any cached or stored content. Trinity Cyber may independently communicate with any account owner whose account(s) are associated with your API Client and developer credentials to provide notice of the termination of your right to use an API.

c. Surviving Provisions

When the Terms come to an end, those terms that by their nature are intended to continue indefinitely will continue to apply, including but not limited to: Sections 6b, 7, 9, 10, and 11.

Section 10: Liability and No Warranty

a. WARRANTIES

EXCEPT AS EXPRESSLY SET OUT IN THE TERMS, NEITHER TRINITY CYBER NOR ITS SUPPLIERS OR DISTRIBUTORS MAKE ANY SPECIFIC PROMISES ABOUT THE APIS. FOR EXAMPLE, WE DON'T MAKE ANY COMMITMENTS ABOUT THE CONTENT ACCESSED THROUGH THE APIS, THE SPECIFIC FUNCTIONS OF THE APIS, OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. WE PROVIDE THE SERVICE "AS IS".

SOME JURISDICTIONS PROVIDE FOR CERTAIN WARRANTIES, LIKE THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. EXCEPT AS EXPRESSLY PROVIDED FOR IN THE TERMS, TO THE EXTENT PERMITTED BY LAW, WE EXCLUDE ALL WARRANTIES, GUARANTEES, CONDITIONS, REPRESENTATIONS, AND UNDERTAKINGS. TRINITY CYBER MAKES, AND YOU RECEIVE, NO WARRANTIES, EXPRESS, IMPLIED STATUTORY OR IN ANY COMMUNICATION WITH YOU AND COMPANY SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TRINITY CYBER DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

b. LIMITATION OF LIABILITY

WHEN PERMITTED BY LAW, TRINITY CYBER, AND TRINITY CYBER'S SUPPLIERS AND DISTRIBUTORS, WILL NOT BE RESPONSIBLE FOR LOST PROFITS, REVENUES, OR DATA; FINANCIAL LOSSES; OR INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES.

TO THE EXTENT PERMITTED BY LAW, THE TOTAL LIABILITY OF TRINITY CYBER, AND ITS SUPPLIERS AND DISTRIBUTORS, FOR ANY CLAIM UNDER THE TERMS, INCLUDING FOR ANY IMPLIED WARRANTIES, IS LIMITED TO THE AMOUNT YOU PAID US TO USE THE APPLICABLE APIS (OR, IF WE CHOOSE, TO SUPPLYING YOU THE APIS AGAIN) DURING THE SIX MONTHS PRIOR TO THE EVENT GIVING RISE TO THE LIABILITY.

IN ALL CASES, TRINITY CYBER, AND ITS SUPPLIERS AND DISTRIBUTORS, WILL NOT BE LIABLE FOR ANY EXPENSE, LOSS, OR DAMAGE THAT IS NOT REASONABLY FORESEEABLE.

c. Indemnification

Unless prohibited by applicable law, if you are a business, you will defend and indemnify Trinity Cyber, and its affiliates, directors, officers, employees, and users, against all liabilities, damages, losses, costs, fees (including legal fees), and expenses relating to any allegation or third-party legal proceeding to the extent arising from:

1. your misuse or your end user's misuse of the API's;
2. your violation or your end user's violation of the Terms; or
3. any content or data routed into or used with the API's by you, those acting on your behalf, or your end users.

Section 11: General Provisions

a. Modification

We may modify the Terms or any portion to, for example, reflect changes to the law or changes to our API's. You should look at the Terms regularly. We'll post notice of modifications to the Terms within the documentation of each applicable API and to this website. Changes will not apply retroactively and will become effective no sooner than 30 days after they are posted. But changes addressing new functions for an API or changes made for legal reasons will be effective immediately. If you do not agree to the modified Terms for an API, you should discontinue your use of that API. Your continued use of the API constitutes your acceptance of the modified Terms.

b. U.S. Federal Agency Entities

The API's were developed solely at private expense and are commercial computer software and related documentation within the meaning of the applicable U.S. Federal Acquisition Regulation and agency supplements thereto.

c. General Legal Terms

We each agree to contract in the English language. If we provide a translation of the Terms, we do so for your convenience only and the English Terms will solely govern our relationship. The Terms do not create any third-party beneficiary rights or any agency, partnership, or joint venture. Nothing in the Terms will limit either party's ability to seek injunctive relief. We are not liable for failure or delay in performance to the extent caused by circumstances beyond our reasonable control. If you do not comply with the Terms, and Trinity Cyber does not take action right away, this does not mean that Trinity Cyber is giving up any rights that it may have (such as taking action in the future). If it turns out that a particular term is not enforceable, this will not affect any other terms. The Terms are the entire agreement between you and Trinity Cyber relating to its subject and supersede any prior or contemporaneous agreements on that subject. For information about how to contact Trinity Cyber, please visit our contact page.

File Inspection Platform Terms of Service

Except as set forth below: (i) the laws of Maryland, U.S.A., excluding Maryland's conflict of laws rules, will apply to any disputes arising out of or related to the Terms or the API's and (ii) ALL CLAIMS ARISING OUT OF OR RELATING TO THE TERMS OR THE APIS WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF PRINCE GEORGE'S COUNTY, MARYLAND, USA, AND YOU AND TRINITY CYBER CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

If you are accepting the Terms on behalf of a United States federal government entity, then the following applies instead of the paragraph above: the laws of the United States of America, excluding its conflict of laws rules, will apply to any disputes arising out of or related to the Terms or the API's. Solely to the extent permitted by United States Federal law: (i) the laws of the State of California (excluding California's conflict of laws rules) will apply in the absence of applicable federal law; and (ii) FOR ALL CLAIMS ARISING OUT OF OR RELATING TO THE TERMS OR THE APIS, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

If you are accepting the Terms on behalf of a United States city, county, or state government entity, then the following applies instead of the paragraph above: the parties agree to remain silent regarding governing law and venue.

NOTE: For trial demonstrations of the Service for which Trinity Cyber does not charge a fee and for temporary credentials issued for free trial access to the file inspection platform service the above requirements to pay an access fee do not apply.

Last Update: January 25, 2022