Endpoint Security AV | Cylance

1. Definitions

In this section:

(a) **Anonymous Data** means a cryptographic hash used and distributed by Cylance to promote awareness, detection and prevention of internet security risks, which will be without attribution to the Customer, or to its operations, systems or networks;

(b) **Documentation** means any published documentation and user manual accompanying delivery of the Software; and

(c) **Software** means Cylance’s proprietary solution, as identified in this Proposal, including any endpoint component(s), online components, proprietary analytical engines, and any related API Material, web interfaces, virtual machines, applications, programs, license keys, installer software, Documentation or any content delivered or made available as part of the solution, and further including any copies of the foregoing made by Cenitex, and any upgrades or modifications of the foregoing delivered by Cylance to Cenitex.

2. Access and use of the Cylance Software

The Customer may:

(a) install and run the Software (end point components delivered):

(1) during the Services Term only (if any);

(2) in object code format only;

(3) on computers owned or controlled solely by the Customer; and

(4) solely to process data solely owned or controlled by the Customer for internal operations and internal data processing purposes; and

(b) access and use the Services solely in support of the rights granted in this clause.

3. Restrictions on use

(a) The Customer may not directly or indirectly (nor authorise any person or entity to):

(1) sell, rent, lease, distribute, redistribute or transfer the Software or any rights in any of the Software, or use the Software in a hosted or managed services environment except as hosted by Cylance through the Service;

(2) reverse engineer, decompile, disassemble or re-engineer, except and only to the extent that such activity is expressly permitted by applicable law, or otherwise create or attempt to create or permit, allow, or assist others to create or derive the source code of the Software, or its structural framework;

(3) modify or create derivative works of the Software;

(4) use the Software or Service in whole or in part for any purpose except as expressly provided under this section;

(5) remove any proprietary notice, labels, or marks on or in Software;

(6) disable or circumvent any access control or related device, process or procedure established with respect to the Software; or

(7) disclose the results of any benchmark tests or other tests connected with the Software to any third party without the prior written consent of Cylance.

(b) While using the Service, the Customer may not directly or indirectly, nor authorise any person or entity to:

(1) access or use (or attempt to access or use) the account of another user without permission, or the login information of another user;

(2) “frame” or “mirror” any portion of the Service;

(3) use any robot, spider, site search/retrieval application or other manual or automatic device or process to retrieve, index, “data mine” or in any way reproduce or circumvent the navigational structure or presentation of the Service; or

(4) probe, scan or test the vulnerability of the Service, nor breach the security or authentication measures on the Service, or take any action that imposes an unreasonable or disproportionately large load on the infrastructure of the Service, such as a denial of service attack.

4. Potentially Malicious Code

The Customer acknowledges and agrees that:

(a) a feature of the Software is to facilitate analysis of files and processes (including, but not limited to, portable executable files or other executable code) that exist on, or are being introduced into the Customer's computer systems or networks (**"Files**") to identify potential or actual malicious code, malware or other intrusive artefacts or processes therein ("**Potentially Malicious Code**");

(b) in certain configurations, to function optimally and for purposes in connection with Cylance's support of the Software, the Software may transmit Files to servers owned or controlled by Cylance, and Cylance may otherwise analyse or classify the File;

(c) Cylance may use, copy, modify, distribute and display Files, Anonymous Data and Potentially Malicious Code for its business purposes, including without limitation for developing, enhancing and support products and services. Cylance will not identify the Customer as the source of any Files or Potentially Malicious Code;

(d) if the Software identifies Potentially Malicious Code, certain configurations of the Software may block Potentially Malicious Code from execution, in which case, the Customer may either:

(1) allow the execution of the Code;

(2) block the execution of the Code;

(3) quarantine the Code; or

(4) if the Customer determines that the Potentially Malicious Code is acceptable for use on its systems, and need not be blocked or quarantined, accept that Potentially Malicious Code;

(e) any decision by the Customer to block the execution of, or quarantine or run Potentially Malicious Code, is at the Customer's own risk, and may result in loss of functionality of the Customer's Files, applications or Customer systems and networks, and cause other potential harm or loss; and

(f) Cylance have no control over the specific conditions under which the Customer uses the Software or allows or disallows Potentially Malicious Code to execute.

5. Termination

(a) Upon termination of the Agreement, the Customer must:

(1) uninstall, and cause all of its users to uninstall, all copies of the Software, and cease, and cause all its users to cease, all use of the Software and Services;

(2) upon Cenitex's or Cylance's request, return to Cylance (or destroy) all copies of the Software in the Customer's possession or control; and

(3) upon Cenitex's or Cylance's request, certify in writing its compliance with subclauses (1) and (2) above.

6. Provision of Customer Information

(a) The Customer acknowledges that the Software may collect information about the Customer's systems and applications in connection with the support of the Software, including, without limitations, usernames, filepath, MAC Addresses, network information, hardware type, model number, hard disk size, CPU type, disk type, RAM size, systems architecture, operating system, versions, locale, BIOS version, BIOS model, system telemetry, device ID, IP address, location, information about third party products, and other configurations, settings and artefacts, including metadata related to the execution of Potentially Malicious Code.