SERVICE ATTACHMENT

MANAGED ENDPOINT DETECTION AND RESPONSE WITH CYNET ALL-IN-ONE

Capitalized terms not defined in this Attachment will have the meanings set forth in the MSA.

"Services" will mean SilverSky Managed Endpoint Detection and Response (MEDR) Services with Cynet All-In-One Agent (CAIOA). This service may also be included in the Lightning Complete service as noted in the table below.

Service SKUs:

SKU	Name	Pricing Unit
S-200-3186	SilverSky MEDR with Cynet All-In-One	Per Endpoint
S-200-3208	Lightning Complete MxDR - Endpoint	Per Endpoint

SKU	Name
I-200-3186	Installation of SilverSky MEDR with Cynet All-In-One
I-200-3208	Installation of Lightning Complete MxDR - Endpoint

SilverSky Services

SilverSky Platform to ingest data/events from CAIOA deployed on endpoints and/or server workloads across the customer environment. All ingested events are automatically enriched with threat intelligence data, matched against a variety of Indicators of Compromise and intelligently cross-correlated to detect anomalies across customer infrastructure.

1. 24/7/365 coverage over all actionable incidents routed to our platform; such incidents are reviewed by an Analyst on a 24/7/365 basis. Customers get full visibility into notified and non-notified incidents via our SilverSky Customer Portal.
2. Customer will have access to our global security operations team for incident investigations and real-time support.
3. Customized Playbooks: to provide notifications to identified client contacts via agreed-upon, specified communication formats. We will provide guided remediation and containment based on the managed endpoint controls in the customer environment. Per the playbook, SilverSky will provide containment and rollback efforts as required.
4. Reporting: a set of customizable reports from report templates via the SilverSky Customer Portal ncluding, but not limited to, Executive summaries and threat and compliance reports as well as access to the Cynet CAIOA Portal.
5. Platform transparency by providing customer access directly into the SilverSky Platform and CAIOA console.
6. Data is retained for one year.
7. To deliver these services we are reselling the CAIOA solution. We represent and warrant that we have obtained all required authorizations and consents to resell the CAIOA license to Customer as part of this MSA and agree to defend, indemnify, and hold harmless Customer against any actual or alleged claims, damages, or losses arising from our resale of the CAIOA license to Customer including, without limitation, any claims of infringement or unauthorized use. We further represent and warrant that the CAIOA license is not an early adoption or beta version of the Solution as defined in Cynet end user license agreement. As the end customer of Cynet, you must adhere to all Cynet end-user provisions located at https://www.cynet.com/eula/.
8. Please note that SilverSky is providing endpoint security utilizing the CAIOA. The CAIOA solutions are procured by SilverSky via a Managed Security Service Provider ("MSSP") license and delivered to you as a service. As such, all licensing for this service is controlled by the MSSP licensing agreement between SilverSky and Cynet.
9. The added Cynet Ransomware Warranty attached below is included as a part of the offering

Optional Services

Email Protection is a service that is designed to enhance the basic Microsoft 365 email protection offering. Cynet All-in-One Mail Protection (CAIOMP) is a lightweight email protection suite for small businesses with no other enhanced email protection offering. The service is a plug-in and not an MX redirect to another platform. The current plug-in only works for customers with Microsoft 365 email. This must be requested to be installed at the time of the initial Deployment or a $500 re-installation fee will be required. The CAIOMP includes:

a. **Attachment scanning**
   Verify email attachments are not weaponized with dangerous malware, including the ability to always block specific file extensions
b. **URL scanning**
   Verify embedded links are not connected to phishing or malicious sites, including real-time checking of link targets when opened
c. **Allowlist, Blocklist**
   Set specific senders, recipients, email domains, attachment types, or sha256 file types that are either always allowed or always blocked
d. **Policy controls**
   Intuitive dashboard to set policies, including the option of notifying users of quarantined emails and review all emails that were tagged as malicious for the timeframe selected
e. **Quarantine**

Prevents the malicious email from arriving to inbox while allowing administrator to review and release directly from the console

f. Tag external emails
Flag emails that were sent from a domain that doesn't match the administrator's domain as external emails

g. Automated response
Automatically remediate email threats and notify the administrator

Vulnerability Scanning is a vulnerability scanning service for small businesses that do not have other vulnerability scanning services or only have external scanning services. This service will provide vulnerability scanning on all endpoints on which the Cynet All-in-One Agent is installed and configured for scanning. Every four hours, it will scan each agent to look for vulnerabilities and represent those capabilities in the Cynet Portal. You will see each vulnerability's status from a Critical – High – Medium, and Low rating. The Common Vulnerabilities & Exposures (CVE) will be attached to the vulnerability within the Cynet portal. From that data you can determine the steps needed to address the vulnerability. This must be requested to be installed at the time of the initial Deployment or a $500 re-installation fee will be required.

SERVICE IMPLEMENTATION

SilverSky Responsibilities

1. Conduct a knowledge-sharing survey to collect information about the Customer's environment, including ingestion data types and sources to be monitored and processes needed to support the implementation of services.
2. Establish a secure method of transmitting logs from the Customer network to the SilverSky Platform.
3. Notify the Customer of receipt of logs and confirm proper operational integration to ensure alerting.
4. Provide initial training and training materials for the SilverSky customer portal.

SilverSky Service Deliverables

1. Capture device logs from the Customer's monitored devices.
2. Adjust the configuration and update CAIOA with Customer collaboration.
3. Perform analysis of the log data. This includes but is not limited to, aggregation, parsing, correlation and alerting.
4. In cases of significant risk, SilverSky analysts will analyze incidents following an alert by the risk notification system.
5. Analysts will notify the Customer of incidents requiring a response. Instructions on threat remediation and consultation will be provided, as defined in the Customer playbook created during deployment.
6. 24/7/365 phone and email-based incident support for additional investigation and guidance for the Customer.
7. Implement change requests.

Customer Responsibilities. During the performance of the Services, Customer will:

1. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the MEDR Service.
2. Ensure complete and current contact information is provided on a timely basis.
3. Cooperate during the deployment period, including providing SilverSky with all required information in a complete and accurate form to prevent implementation delays which may result in additional fees.
4. Appoint one or more authorized contacts authorized to approve and validate all requested changes.
5. Provide all necessary information with respect to your environment.
6. Provide the necessary tool to deploy CAIOA on all endpoints in the customer environment and deploy CAIOA.
7. Ensure the format and quality of the data being sent to SilverSky is sufficient for SilverSky to provide the Services.
8. Retain authority and responsibility for decisions made regarding this service implementation.
9. Assume responsibility for any direct or physical remediation.

You acknowledge that your fulfillment of these responsibilities is essential to our ability to perform MEDR Services in a timely manner.

Optional Service - Mobile Protect

This must be requested to be installed at the time of the initial Deployment or a $500 re-installation fee will be required.

SilverSky Platform will ingest security events from the Cynet Mobile Protect (CMP) console utilizing the Zimperium platform for CMP agents deployed on individual mobile devices across the end-customer environment. All ingested events are automatically enriched with threat intelligence data, matched against various Indicators of Compromise (IOC), and intelligently cross-correlated to detect anomalies across customer infrastructure.

SilverSky Responsibilities:

1. Site provisioning. Provision the CMP console for the Customer or Partner. Grant access to the CMP console to the Customer or Partner. Create a threat policy baseline for CMP console.
2. Ingest CMP security events into the Lightning Platform to enable the SilverSky SOC to monitor events and incidents.
3. Confirmation of successful deployment. Once the agent is installed on the end-user mobile devices, SilverSky will confirm that they have been successfully onboarded into the CMP console.
4. Update the CMP console with current threat policies.
5. Monitoring the CMP alerts and notification to the Customer or Partner of suspicious activity to the end customer.
6. Troubleshoot CMP concerns with Cynet vendor.

Customer/Partner Responsibilities:

1. Designate team responsible for the CMP service, with both the capability and authority to execute the changes required on end-user mobile devices, whether direct to end users or businesses at their discretion.
    a. This team will be the sole communication and contact with end-users and SilverSky.
    b. Provide SilverSky with an authorized list of contacts. Note that no end-user is allowed to contact SilverSky directly.
    c. Authorized users will access the CMP console, which is provided by SilverSky, with multi-factor authentication.
2. Provide input to SilverSky on tuning the CMP threat policy related to relevant alert ingestion, policy settings, and mitigation action configuration.
3. If available, integrate CMP with the existing and Cynet-approved Mobile Device Management (MDM) solution, following instructions from SilverSky on integrating with the CMP console. SilverSky is not responsible for setting up, configuring, or troubleshooting MDM issues.
4. Individual device deployment of the CMP agent for Customers:
    a. Provide a list of the full names and email addresses of end-users with mobile devices who will be onboarded for the service.
    b. The end user will follow the steps in the SilverSky email invitation to download and install the agent and establish a connection with the CMP console.
    c. Responsible for adherence to the correct installation and activation of the application.
5. Individual device deployment of the CMP agent for Partners:
    a. Partner will configure the device within the CMP and email instructions to download the agent.
    b. The end user will follow the Partner provided email invitation steps to download and install the agent and establish a connection with the CMP console.
    c. Responsible for adherence to the correct installation and activation of the application.
6. MDM mass deployment automation:
    a. Where an MDM is available to deploy the CMP application, SilverSky will provide App Config Details for automatic activation to the Customer or Partner.
    b. The Customer or Partner is responsible for installing, activating, and confirming a successful connection to the CMP console.
7. Ensuring devices meet the minimum requirements for installation and effective operation of the CMP application
8. Action and verify the successful completion of automatic mobile device updates from the CMP agent
9. Responding to notifications from the SilverSky SOC to security cases published within the Lightning Portal: confirming or denying the legitimacy of the activity through internal review.
10. Performing actions necessary to mitigate any threat identified by SilverSky.
11. Accept the End User License Agreement for each mobile device as part of the CMP application installation. Zimperium End User License Agreement & Privacy Policy

Service Level Agreement for Managed Endpoint Detection and Response

If we fail to meet the levels defined in this MEDR Service Level Agreement (SLA) for a minimum of two (2) consecutive months, you must notify us in writing of any violations and allow us thirty (30) days from notification to cure the breach. If the breach is still unresolved, you may immediately terminate the MEDR Service, giving rise to such breach without additional notification or incurring early termination fees within thirty (30) days of our failure to cure.

1. **Service Hours of Operation.** We maintain Security Operations, Network Operations, and Technical Support departments 24 x 7 x 365. You may reach an individual in each department by calling the appropriate support service.

2. **Response Time.** We commit to certain incident response times. These commitments are subject to your providing us with accurate and current contact information for your designated points of contact. Our failure to respond in accordance with the parameters defined herein will entitle you to receive, as your sole remedy and our sole obligation, credits described below, *provided, however*, that you may obtain no more than one credit per day, regardless of how often in that day we failed to meet these parameters.

3. **Event and Case Severity Classification**—SilverSky will facilitate communication with the Customer through one of SilverSky's approved notification methods (email, phone, or SilverSky Portal). Customers can customize their preferred notification methods within their customized playbooks within the SilverSky Portal. To classify the severity of the items, SilverSky will follow the definitions of the Case Severity in the table below. Events form the basis from which the SilverSky analyst may begin their investigation. An Event is the initial alert level generated from the source device as indicated through the SilverSky platform. An Event is assigned to SilverSky analysts, who will perform the initial investigation to determine the Case Severity defined below. The Case, as defined by the SilverSky analyst, is the process through which a SilverSky analyst reviews and performs an investigation to confirm the validity of an Event. During the investigation, the SilverSky analyst will acknowledge the Event, assess the potential impact, and assign the appropriate Case Severity. Once the Case Severity has been validated, it will be the trigger point to begin the SLA measurements. The following SLAs have been established to initiate communication with the Customer that the SOC has initiated an investigation or actions. SLAs are measured from the start of the Case Severity determination until the time the Customer is notified. Customer notifications occur after Case Severity determination to reduce the potential notification for benign or false positive events. Mean time to acknowledge is the official measurement of this SLA and is measured as the time period from Case status change from "New" to "Opened" within the SilverSky Portal until the Customer receives notification per their communication plan as outlined below.

Case Severity	Definition	Service Level	Notification Methods
Critical	This Case category may severely impact your network or system and indicate a compromise. Examples of Cases that fall under this category are confirmed ransomware, infiltration, and lateral movement.	**10 minutes from Case creation**	• **Email** • **Phone Call** • **SilverSky Portal**
High	This Case category may have a high impact on your network or system. It could lead to malware infection, data leakage, and disruption of operations due to network or system downtime. Examples of Cases that fall under this category are suspected compromise, suspected initial access, known malware installations (blocked or not), and ongoing attacks.	**30 minutes from Case creation**	• **Email** • **Phone Call** • **Lightning Portal**
Medium	This Case category has a medium impact on your network or system and could lead to unnecessary information leakage or vulnerability exposure. Examples of Cases that fall under this category are excessive login failures, scanning/firewall blocks, suspicious privileged access, and impossible travel.	**48 hours from Case creation**	• **Lightning Portal**
Low	This Case Category has little impact on the Customer. Examples of Cases that fall under this category are access creation/changes, reported phishing emails, and unexpected behavior.	**72 Hours from Case creation**	• **Lightning Portal**

Case Severity	Definition	Service Level	Notification Methods
Informational	This Case category shows no impact on the Customer. These are only informational to track activity. Examples of Cases that may fall under this category are false positives, system error messages, and audit-purposes event logs.	**No SLA**	• **Lightning Portal**

4. **Service Requests:** Service Requests are items that are not related to an Event or a Case and may be submitted by the Customer through the SilverSky Portal, Email, or telephone. These requests are not subject to SLA criteria.

5. **Service Availability Guarantee:** We commit to making services under this agreement available 99.5% of the time. At your request, we will calculate the number of minutes the Service(s) was unavailable to you in a calendar month ("Service Unavailability").

5.1. **Customer Service Outage** – The SLA shall not apply in the event of any Customer-caused Service outage that prohibits or otherwise limits SilverSky from providing the Service delivering the SLAs, including, but not limited to, Customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software Devices by Customer, its employees, agents, or third parties acting on behalf of Customer.

5.2. **SLA Credits—**You must be current with your payments when the missed SLA event occurs to receive credit under an SLA. In addition, all credit requests must be submitted in writing through the SilverSky Portal, email, or certified U.S. mail. You must submit each request for credit within seven (7) days of the occurrence giving rise to the credit claim. SilverSky will research the request and respond to the Customer within thirty (30) days from the date of the request.

The total credit amount we will pay to you in any calendar month will not exceed, in the aggregate, half of the total fees invoiced to you for the Lightning Managed Detection and Response Services for which a claim is made in the applicable month. (Credits are exclusive of any applicable taxes charged to you or collected by us.) Unless otherwise expressly provided hereunder or in the MSA, the foregoing SLA credit(s) shall be the Customer's exclusive remedy for failure to meet or exceed the foregoing SLAs.

6. **Credit Calculation:**

- If SilverSky fails to meet one SLA in a calendar month, then Customer will be entitled to a service credit equal to 1/30th of the monthly fee for Service for each calendar day upon which the SLA was not met.
- If SilverSky fails to meet more than one but less than four SLAs in a calendar month, then the Customer will be entitled to a service credit equal to 1/5 of the monthly fee for Service for each calendar day upon which the SLAs were not met.
- If SilverSky fails to meet more than three SLAs in a calendar month, then the Customer will be entitled to a service credit equal to 1/2 of the monthly fee for Service for that month.

Service credits may not exceed 50% of the monthly service fees for the applicable services.

7. **Maintenance Windows** – SilverSky may schedule maintenance outages for any portion of services within 24 hours' notice to designate Customer contacts. SLAs shall not apply during maintenance outages and, therefore, are not eligible for SLA credit during these periods. SilverSky will make every attempt to adhere to its weekly maintenance windows for service outages. SilverSky Standard Maintenance windows are

- Tuesday and Thursday (12 AM – 2 AM ET)
- Saturday (12 AM – 5 AM ET)

Emergency Maintenance – In the circumstance of immediate necessary changes, SilverSky may initiate an emergency maintenance window. When this situation occurs, SilverSky will use commercially reasonable efforts to provide notice and minimize the impact to customers.

8. **Exceptions**: You will not receive any credits under this SLA regarding any failure or deficiency of the Services or a failure to meet service level caused by or associated with any of the following:

- Maintenance, as defined above;

- Fiber cuts or other such issues related to telephone company circuits or local ISPs outside of our control;
- Third-Party Outages—This is for the log collection of third-party sources such as software-as-a-service, Cloud infrastructure providers, or third-party tools that SilverSky does not control.
- Your applications, equipment, or facilities failures;
- You or any of your end-users' acts or omissions;
- Reasons of Force Majeure as defined in the Terms and Conditions associated with this MSA;
- Any act or omission on the part of any third party not reasonably within our control;
- First month of service for the specific Managed Detection and Response Services for which a credit is claimed;
- DNS issues outside our direct control;
- Broadband connectivity.

9. Fair Usage Threshold for Data Ingestion: SilverSky maintains a fair usage policy to ensure the availability and sustainability of the Service. Failure to adhere to the fair usage policy will result first in a notification to you and then, if you fail to take remedial action, suspension of this SLA until such time as the usage level associated with the corresponding data sources falls below a reasonable, standard threshold.

10. Data Retention Policy

SilverSky ensures the archival and retention of all security logs ingested into our system across various supported platforms. Data is categorized into three storage tiers: Hot, Warm, and Cold. Each tier has specific retention periods and accessibility features as outlined below so that all logs are maintained within the SilverSky platform for at least 365 days:

1. **Hot Data** refers to security logs actively used for daily security or operational investigations or to establish baselines for identifying malicious activity. This data is readily searchable and available in near real-time to support ongoing investigations.
    - Retention Period: 30 days
2. **Warm Data** encompasses security logs retained for further enrichment and analysis. These security logs are typically used in active threat-hunting investigations to detect trends and patterns over an extended period. Warm data provides contextual information to support security or operational activities and is accessible within minutes to hours.
    - Retention Period: 90 days
3. **Cold Data** consists of security logs stored for long-term compliance, historical reference, or incident investigation. This data is preserved for extended periods and can be restored for forensic analysis when required. Cold data is accessible upon customer request for restoration, typically within 48 hours of the request.
    - Retention Period: 121 thru 365 days

SilverSky's data retention policy is designed to ensure that logs are available for appropriate use while balancing performance and compliance requirements.

11. Additional Disclaimers. We do not guarantee a continuous, uninterrupted, virus-free, malware-free, intrusion-free, or continuously secure Customer network or network environment, and we are not liable if you or your end users are unable to access your network at any specific time. Additionally, we do not guarantee that we will be able to replace any of your information, content, or other data that may be lost, damaged, or stolen resulting from use of the Services.

Appendix A – Definitions

SilverSky SOC Escalation terms

All Response activity is governed by an escalation method where SilverSky escalates information we receive from your systems as follows.

Syslog: Protocol used to collect raw logs from customer devices to SilverSky collector.

Event: Raw information received from your organization

Alert: An event or group of events that have an indication of out-of-policy, known activity signature match, or other anomalous behavior.

Case: A single alert or a group of alerts grouped or cross correlated together.

CYNET RANSOMWARE WARRANTY

This Ransomware Warranty (the "**Warranty Agreement**") is entered into by Cynet Security Ltd. and/or any of its Affiliates ("**Cynet**") and the Customer (as defined below).

In consideration of the mutual obligations outlined, the Parties agree that the following terms and conditions shall form an Addendum to the Sales Order (as defined below).

1. Definitions

1.1. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

1.2. "**Agent**" means any optional piece of software code Cynet provides the Customer (directly or via a Partner) (whether downloadable from Cynet Servers and/or deployed from the installation package installed with the Platform), and installed on all, selected, or none, of Customer's End Points.

1.3. "**Agreement**" means this Warranty Agreement together with the Sales Order that was executed by Cynet and/or any of its Affiliates and the Customer or the Partner (as applicable).

1.4. "**Business Day**" means a normal working day and excludes weekends and public holidays.

1.5. "**By-standing Cyber Asset**" means a Computer System used by the Customer or its third-party service providers that is not physically located in an Impacted State but is affected by a Cyber sys.

1.6. **"BYOD"** means bring your own device.

1.7. "**Computer System**" means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.

1.8. "**Customer**" means a legal entity which is granted with a subscription to the Platform, under a Sales Order, whether directly or via a Partner. For the purpose of Customer's acts and/or omission and/or undertakings the term Customer shall also include anyone on Customer's behalf (including but not limited, to employees, contractors, etc.). For avoidance of doubt, for the purpose of this Warranty Agreement, a Customer shall also include any of the following: (i) Affiliate(s) of the Customer, which is using the Platform under Customer's subscription; (ii) a Managed Security Service Provider (MSSP) or a Managed Service Provider (MSP), who has a valid MSSP/MSP Agreement with Cynet.

1.9. "**Cyber Operation**" means the use of a Computer System by or on behalf of a State to disrupt, deny, degrade, manipulate or destroy information in a Computer System of or in another State.

1.10. "**Eligible Endpoint**" means any and all Endpoints on which the most recent release of the Platform (which was made available to the Customer) is installed and provided further that the operating system of the Endpoint is supported by the Platform.

1.11. "**Endpoint**" means any physical or virtualized computing device which is managed by, and/or associated to (for BYODs only) the Customer. For the purposes of these terms, Endpoints include mobile devices, desktop computers, laptops, virtual machines, and servers.

1.12. "**Essential Service**" means a service that is essential for the maintenance of vital functions of a State including without limitation: financial institutions and associated financial market infrastructure, health services or utility services.

1.13. "**EULA**" means Cynet's most current terms and conditions which are currently available at <www.Cynet.com/eula>.

1.14. "**Discovery Date**" means the first date in which the Customer was made aware of the Ransomware Event.

1.15. "**File**" means a container in a computer system for storing information

1.16. "**Impacted State**" means any State where a Cyber Operation has had a major detrimental impact on: the functioning of that state due to the direct or indirect effect of the Cyber Operation on the availability, integrity or delivery of an Essential Service in that State; and/or the security or defense of that State.

1.17. "**Infected Eligible Endpoint**" means an Eligible Endpoint directly affected by a Ransomware Event resulting in destruction and/or irreversible encryption of its data.

1.18. "**Parties**" means the Customer and Cynet collectively.

1.19. "**Partner**" means any of Cynet's approved distributor and/or reseller which is authorized by Cynet to grant Customer with access to the Platform.

1.20. "**MSSP/MSP Agreement**" means an agreement executed by the MSSP/MSP with Cynet.

1.21. "**Pre-existing Event**" means any unauthorized access to any Eligible Endpoint of the Customer which occurred either (i) prior

to the Warranty Period or (ii) prior to Customer's Endpoint becoming an Eligible Endpoint.

1.22. "**Platform**" means the Cynet AutoXDR platform

1.23. "**Ransomware Event**" means the unauthorized access of a third party to an Eligible Endpoint, consisting of a malware specifically utilizing encryption-ware measures and attempting to encrypt data stored on the Eligible Endpoint, all for the purpose of demanding payment of ransom from the Customer, where the Platform had failed to detect and prevent the occurrence of such unauthorized access. It is hereby clarified that any access by any of the Customer's representatives (such as employees, consultants, contractors, service providers etc.) will not be considered as an unauthorized access and as such shall not be considered as a Ransomware Event.

1.24. "**Sales Order**" means an order form submitted to or by a Customer or a Partner (as applicable) which must include, subscription to the Platform, Ransomware Warranty coverage, number of Endpoints, pricing, payment terms and the like and which was duly approved by Cynet, the Customer or the Partner (as applicable).

1.25. "**Specified States**" means China, France, Germany, Japan, Russia, UK or USA.

1.26. "**State**" means sovereign state.

1.27. "**War**" means the use of physical force by a State against another State or as part of a civil war, rebellion, revolution, insurrection, and/or military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority, whether war be declared or not.

1.28. "**Warranty Period**" means the period in which the subscription of the Customer to the Platform is in effect, as set forth in the Sales Order and provided further that the Ransomware Warranty is included in such order. The Warranty Period for each Warranty shall be a maximum of 12 months from its inception. Any renewal or extension of a Warranty shall result in a new inception of that Warranty, for which the abovementioned Warranty Period conditions apply.

2. The Warranty

2.1. If during the Warranty Period, Customer suffers a Ransomware Event that results in an Eligible Endpoint(s) becoming an Infected Eligible Endpoint(s), then subject to the terms and conditions of this Warranty Agreement, Cynet shall pay the Customer the lower of (i) USD 1,000 per each Infected Eligible Endpoint or
(ii) three (3) times the annual fee as set forth in the respective Sales Order (the "**Pay Out**").

2.2. This Warranty Agreement applies solely to Eligible Endpoint(s).

2.3. Notwithstanding anything to the contrary, in no event during the Warranty Period shall the Customer receive from Cynet in aggregate more than USD 1,000,000 (USD One million) and no more than one payment for each Infected Eligible Endpoint (the "**Warranty Cap**").

2.4. The aggregate coverage under this Warranty Agreement for the Customer, including its Affiliates, shall not exceed the Warranty Cap.

2.5. The Pay Out sets forth Customer's sole and exclusive remedy under this Warranty Agreement.

3. Exclusions

All the Sections of this Warranty Agreement are subject to the following exclusions. This Warranty Agreement excludes coverage for any loss, damage, liability, cost, or expense arising directly or indirectly from:

3.1. Files that are not on the Eligible Endpoint;

3.2. Any deployment, configuration and/or use of the Platform (or a portion thereof), for any or no reason, in a manner inconsistent with the Documentation (as such term is defined in the EULA).

3.3. There were pending actions (such as reboot) listed on any Eligible Endpoint prior and/or during the Ransomware Event

3.4. Pre-existing Event;

3.5. Files white-listed by the Customer and/or anyone on its behalf;

3.6. Endpoint which is not protected by the Platform;

3.7. Endpoint on which the most recent release of Platform is not installed;Failure by the Customer to set the Platform and/or any of the Endpoint(s) in accordance with Cynet's best protection practices (as may be amended from time to time) as were communicated to the Customer in the form of documentation, Cynet staff guidance, training, and other means;

3.8. Failure by the Customer to implement best industry practices in relation to the operation and overall security of the Endpoints (including the Eligible Endpoints), that if used, might have prevented the occurrence of the Ransomware Event which is covered under this Warranty Agreement;

3.9. Failure by the Customer to take a remediation and rollback action within two (2) hours as of the first time the Customer was made aware of the Ransomware Event;
3.10. Events occurring in connection to a device which has been exposed to abnormal physical or electrical stress, misuse, negligence or accident;
3.11. Failure by the Customer to comply with Cynet's suggestions and/or mitigation plan(s);
3.12. The Ransomware Event occurred prior or after the Warranty Period;
3.13. The Customer notified Cynet about the Ransomware Event after the Warranty Period;
3.14. The Endpoint was not malware free prior to the installation of the Agent;
3.15. Customer (and/or the Partner as applicable) is in breach of any of its undertaking under this Warranty Agreement and/or the EULA and/or under the Sales Order (including without limitation, payment obligations);
3.16. Failure to update and/or install the latest security updates which are available for the operating system of the Endpoint;
3.17. VSS (Volume Shadow Copy Service) is not enabled and does not function on all Endpoints (which Windows is their operating system). VSS Disk Space Usage allocation is not configured with at least 10% on all disks.
3.18. Failure to update and/or install the latest security updates which are available for any software which is installed on any Endpoint;
3.19. Customer's negligence or misconduct;
3.20. Pay-Out will cause Cynet to violate any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, the United Kingdom or United States of America, or any violation of any regulation or specific national law applicable to Cynet;
3.21. Other products and/or services which directly or indirectly cause the malfunction or non-performance of the Platform with respect to the subject Ransomware Event;
3.22. War or a Cyber Operation that is carried out in the course of War;
3.23. Retaliatory Cyber Operations between any Specified States leading to two or more Specified States becoming Impacted States;
3.24. A Cyber Operation that has a major detrimental impact on the functioning of a State due to the direct or indirect effect of the Cyber Operation on the availability, integrity or delivery of an Essential Service in that State; and/or the security or defence of a State. This exclusion shall not apply to the direct or indirect effect of a Cyber Operation on a By-standing Cyber Asset.

4. Limited Warranties

OTHER THAN AS EXPLICITLY STATED IN THIS WARRANTY AGREEMENT AND THE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE PLATFORM, IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, AND CUSTOMER ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT CYNET DOES NOT GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF CUSTOMER'S OR ITS AFFILIATES' SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE, AND CUSTOMER AND ITS AFFILIATES WILL NOT HOLD CYNET RESPONSIBLE THEREFOR. CYNET DOES NOT WARRANT THAT: (I) THE SERVICES WILL MEET CUSTOMER'S REQUIREMENTS, OR (II) THE PLATFORM WILL OPERATE ERROR-FREE. CYNET EXPRESSLY DISCLAIMS ALL EXPRESS WARRANTIES AND ALL IMPLIED OR STATUTORY WARRANTIES, INCLUDING MERCHANTABILITY, TITLE, NON-INFRINGEMENT, NONINTERFERENCE, OR FITNESS FOR A PARTICULAR PURPOSE. THE PLATFORM IS NOT FAULT- TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THE PLATFORM IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY, OR PROPERTY DAMAGE.

Notices

4.1. If during the Warranty Period the Customer is made aware of a Ransomware Event, Customer shall notify Cynet of such event by sending an email to warranty@cynet.com no later than within twenty-four (24) hours after the Discovery Date. In the event that Cynet is made aware of a Ransomware Event, it shall notify the Customer about such event as soon as reasonably possible (the "**Notification Date**").
4.2. Customer shall have twenty (20) days from either: (i) the Discovery Date or (ii) the Notification Date, to request Pay Out by sending an email to warranty@cynet.com (the "**Pay Out Request**").

5. Pay Out Request

5.1. Any Pay Out request under this Warranty Agreement, shall be provided in the following manner: The Customer shall provide Cynet with the following information: (i) total number of Infected Eligible Endpoints;
5.2. (ii) Host name, a MAC address and Hard Drive Serial number of any Infected Eligible Endpoints; (iii) Evidence of Ransomware Event; (iv) Any other relevant documentation and/or information in Customer's possession or control in relation to the Ransomware

Event and (v) a statement executed by an authorized individual of the Customer in the form such forth in Exhibit A.

5.3. During the Warranty Period and for a period of three (3) years thereafter, Cynet shall have the right at its own expense to inspect, and Customer shall maintain and provide, Customer's records related to such Ransomware Event upon reasonable written request during regular business hours.

6. Pay Out Procedures

6.1. Cynet will review the Pay-Out Request, and the Customer shall provide any additional information reasonably requested by Cynet.

6.2. By submitting the Pay Out Request, Customer authorizes Cynet to share any information that is reasonably necessary to assess the validity of such request with any of its partners which is relevant for the provision of the warranty herein.

6.3. If the total amount of the Pay Out Request **is more than USD 100,000** per Ransomware Event, Cynet shall acknowledge such request within 45 Business Days after such request was submitted by the Customer, and shall make payment on such request within 30 Business Days after the required internal verifications of such request have been cleared and approved.

6.4. If the total amount of the Pay Out Request **is less than USD 100,000** per Ransomware Event, Cynet also shall acknowledge such request no later than 45 Business Days after. such request was submitted by the Customer, and shall make payment on such request, within 30 Business Days after the required internal verifications of such request have been cleared and approved at the end of the quarter.

6.5. For clarity, any payment made by Cynet under this Warranty shall be made solely to the Customer and not to any of its Affiliates.

6.6. If a Pay Out Request arises out of an event that is later determined (i) not to be a Ransomware Event, or (ii) relates to a Pre-Existing Event, Customer shall promptly (but in no event later than **fifteen (15)** days after written notice) reimburse Cynet for all payments actually made by Cynet in relation to such request.

6.7. If Customer failed to provide sufficient proof as set forth in Section 6 above no payment under this Warranty Agreement shall be made to the Customer.

7. Term and Termination

7.1. This Warranty Agreement shall be in effect during the Warranty Period.

7.2. Notwithstanding anything to the contrary, this Warranty Agreement, shall terminate immediately upon the termination of the Sales Order.

7.3. It is hereby clarified that the termination of this Warranty Agreement shall not terminate the Sales Order.

8. No Third-Party Beneficiary

The provisions of this Warranty Agreement are intended to bind the Parties as to each other and are not intended to and do not create rights in any other person or entity or confer upon any other person or entity any benefits, rights or remedies, and no person or entity is or is intended to be a third party beneficiary of any of the provisions of this Warranty Agreement.

Miscellaneous

8.1. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

8.2. If any provision of this Warranty Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

8.3. Neither party may assign its rights or obligations under this Warranty Agreement without the prior written consent of the other party, which consent may not be unreasonably withheld or delayed. Notwithstanding the foregoing, this Agreement may be assigned by either party in connection with a merger, consolidation, sale of all of the equity interests of the party, or a sale of all or substantially all of the assets of the party to which this Warranty Agreement relates. This Warranty Agreement is binding upon and inures to the benefit of the Parties and their respective successors and assigns.

8.4. This Warranty Agreement and any exhibits attached or referred hereto represents the entire agreement of the Parties with respect to the subject matter hereof and supersedes and replaces all prior and contemporaneous oral or written understandings and statements by the parties with respect to such subject matter.

8.5. For any Customer who is a US entity, this Warranty Agreement shall be governed exclusively by the laws of the State of New York, without reference to its conflict of laws principles and the Parties consent to exclusive jurisdiction and venue in and for New York, New York. For any Customer which is domiciled in Europe, this Warranty Agreement shall be governed exclusively by the laws of England and Wales, without reference to its conflict of laws principles and the Parties consent to exclusive jurisdiction and venue in and for London, England. For all other Customers, this Warranty Agreement shall be governed

exclusively by the laws of the State of Israel, without reference to its conflict of laws principles and the Parties consent to exclusive jurisdiction and venue in and for Tel Aviv, Israel.

Exhibit A

Statement

I, the undersigned acting on behalf of _____ [full legal name of the Customer] (the "**Customer**"), in relation to a Pay-Out Request dated _____, hereby confirm that to the best of my knowledge and belief, the information furnished by the Customer in relation to Customer's Pay-Out Request is true and correct in all material respects and no material fact relating to the Ransomware Event has been withheld.

Executed on this ____ day of _____

_____

By: _____ Name:
_____ Title:

_____
Signature