SILVERSKY
Change the Rules of Engagement

SERVICE ATTACHMENT

MANAGED ENDPOINT DETECTION AND RESPONSE FOR MICROSOFT DEFENDER ENDPOINTS

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 for Microsoft Defender Endpoints.

Service SKUs:

SKU	Service Name	Pricing Unit
S-200-3142	MEDR for Defender Endpoints	Endpoint

SKU	Service Name	Pricing Unit
I-200-3142	Installation of MEDR for Defender Endpoints	Per Company
I-201-3142	Audit Review Existing/Customer deployed agents - taking over management	Per Company
I-202-3142	MDE third-party RMM	Per Company

SilverSky Services

SilverSky Platform to ingest data/events from the Microsoft Defender Endpoints 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 Lightning 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 customer portal including, but not limited to, Executive summaries and threat and compliance reports.
5. Platform transparency by providing customer access directly into the SilverSky Platform through the customer portal.
6. Data is retained for one year.

MEDR FOR MICROSOFT DEFENDER ENDPOINTS 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 Microsoft environment 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 Defender Endponts 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. Provide all Microsoft Defender Endpoint licenses
2. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the MEDR for Defender Endpoints.
3. Ensure complete and current contact information is provided on a timely basis.
4. 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.
5. Appoint one or more authorized contacts authorized to approve and validate all requested changes.
6. Provide all necessary information with respect to your environment.
7. Provide the necessary tool to deploy Defender Endpoints on all endpoints in the customer environment and deploy Defender Endpoints.
8. Ensure the format and quality of the data being sent to SilverSky is sufficient for SilverSky to provide the Services.
9. Retain authority and responsibility for decisions made regarding this service implementation.

10. Assume responsibility for any direct or physical remediation.

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

Service Level Agreement for MEDR for Defender Endpoints

Service Level Agreement for Managed Endpoint Detection and Response

If we fail to meet the levels defined in this MEDR for Defender Endpoints 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 for Defender Endpoints 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**

Case Severity	Definition	Service Level	Notification Methods
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**
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.