SERVICE ATTACHMENT FOR
SECURITY DEVICE MANAGEMENT SERVICES

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

1. **"Security Device Management Services"** will mean SilverSky services including principal network security controls in a single-bundled package. This package includes Managed Firewall, Intrusion Detection Prevention Services (IDPS), Web Content Filtering, Gateway AV, remote access that may include two-factor SSL VPN, site-to-site VPNs, and SDWAN (Fortinet). SilverSky provides full management, monitoring, and response for the services, access to configurable reports through the portal, and Lifecycle and Patch Management.

Service SKUs:

SKU	Service Name	Pricing Unit
S-500-3067	SilverSky Security Device Management up to 250MB thruput with FortiGate 6X Series	Per Device
S-501-3067	SilverSky Security Device Management up to 500MB thruput with FortiGate 8X Series	Per Device
S-502-3067	SilverSky Security Device Management up to 1GB thruput with FortiGate 10X Series	Per Device
S-503-3067	SilverSky Security Device Management up to 3GB thruput with FortiGate 20X Series	Per Device
S-500-3068	SilverSky Security Device Management up to 250MB thruput - no hardware included	Per Device
S-501-3068	SilverSky Security Device Management up to 500MB thruput - no hardware included	Per Device
S-502-3068	SilverSky Security Device Management up to 1GB thruput - no hardware included	Per Device
S-503-3068	SilverSky Security Device Management up to 3GB thruput - no hardware included	Per Device
S-200-2182	Site to Site VPN Tunnels	Per VPN
S-200-2866	Secure Identity Soft Tokens for VPN Remote User Access (Block of Five)	Per 5 Tokens

SKU	Service Name
I-500-3067	Installation of SilverSky Security Device Management up to 250MB thruput with FortiGate 6X Series
I-501-3067	Installation of SilverSky Security Device Management up to 500MB thruput with FortiGate 8X Series
I-502-3067	Installation of SilverSky Security Device Management up to 1GB thruput with FortiGate 10X Series
I-503-3067	Installation of SilverSky Security Device Management up to 3GB thruput with FortiGate 20X Series
I-500-3068	SilverSky Security Device Management up to 250MB thruput - no hardware included
I-501-3068	SilverSky Security Device Management up to 500MB thruput - no hardware included
I-502-3068	SilverSky Security Device Management up to 1GB thruput - no hardware included
I-503-3068	SilverSky Security Device Management up to 3GB thruput - no hardware included
I-200-2182	Installation of Site to Site VPN Tunnels
I-200-2663	Installation of Secure Identity Soft Tokens for VPN Remote User Access (Block of Five)

2. **Customer Responsibilities.** During the performance of the Security Device Management Services, you agree to perform the following obligations and acknowledge and agree that SilverSky's ability to perform its obligations, and its liability under the SLAs below, are dependent upon Your compliance with the following:

I. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the Security Device Management Services;

II. Ensure complete and current contact information is provided on a timely basis;

III. Cooperate during the deployment period, including providing us all required information in a complete and accurate form to prevent implementation delays which may result in additional fees;

IV. Appoint one or more authorized contacts authorized to approve and validate all requested changes;

V. Implement change requests;

VI. Provide all necessary information with respect to your environment and communicate any network or system changes that could impact service delivery;

VII. Provide necessary hardware along with maintenance and support contracts to run log collectors within your environment;

a. You are responsible for ensuring that all customer-provided hardware is not EOL and is able to support current software versions.

b. In the event of hardware failure of your owned equipment, You are responsible for initiating and fulfilling the return materials authorization ("RMA") process with the vendor and SilverSky

VIII. Send log data in an encrypted manner, or via the agreed log collection device/type;

IX. Ensure that the format and quality of the data being sent to SilverSky is sufficient enough for SilverSky to provide the Security Device Management Services.

X. Customer is required to provide, configure and manage required switches to support high Availability (HA) mode.

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

3. **SilverSky Deliverables.** During the performance of the Security Device Management Services, SilverSky will configure and deploy the selected security technology and will provide:

I. Continuous 24x7 device availability management (continuous health and security of your managed appliance)

II. A reporting platform to view and audit the alert response process (platform has integrated dashboards, incident management, and flexible reporting)

III. Service support 24x7 with online ticketing

IV. Threat intelligence correlation across the customer firewall and IDPS

V. A Security Management Center (SMC) Portal; portal with reporting functionality on Firewall, Web Content Filter, VPN, and Intrusion Detection Prevention System (IDPS) logs

a. Management of Firewall policies includes adding, deleting, or modifying individual Network Address Translations (NAT) (incoming, outgoing, and loop-back) including object creation

b. Adding, deleting, or modifying access control list changes (such as permit or deny changes) Including the creation of policy objects creation (Hosts, Groups, Networks, Ranges, and Service objects)

c. Adding, deleting, or modifying individual network routes within the firewall

d. Adding, deleting, or modifying IDPS signatures, not including routine signature updates

e. Standard policy change may comprise one or more of the above bullets. SilverSky reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of Customer's service.

VI. Software Upgrades and Patch Maintenance (coordinated with the Customer)

a. In cases where support for a particular product or product version is being discontinued by the vendor or by SilverSky, SilverSky will communicate new platform migration options, if any. To be assured of uninterrupted service, the Customer must complete the migration process within sixty (60) days of notification by SilverSky.

b. For customer-provided hardware, the Customer bears any costs relating to procuring new hardware or components and to re-provisioning any devices.

c. For customers who receive hardware as a part of their service, SilverSky will provide replacement hardware.

VII. Gateway Anti-Virus support (Fortinet). SilverSky will work with Fortinet to update anti-virus signatures/policies regularly when updates are released by Fortinet and reviewed by SilverSky.

VIII. Web Content Filtering (WCF) support (Fortinet). WCF as a licensed option is included in the purchase of this bundle, SilverSky shall deploy the default categorization policy by zone or internet protocol ("IP") range as specified by the customer. Websites that are accessed that are within an enabled category shall not be blocked.

a. Customers can self-manage their WCF actions through the SMC portal or by sending in a change request to SilverSky Support. This is equated to a standard policy change request. Requests for whitelisting or blacklisting of domains are permitted under a standard policy change request.

4. Equipment. Equipment provided to you by us **("SilverSky Equipment")** is for your use only during the Term of this Attachment. We will service the SilverSky Equipment in accordance with our service policies. You agree to (i) use SilverSky Equipment only for the purpose of receiving Security Device Management Services; (ii) prevent any connections to SilverSky Equipment not expressly authorized by us; (iii) prevent tampering, alteration, or repair of SilverSky Equipment by any persons other than us or our authorized personnel; and (iv) assume complete responsibility for improper use, damage to or loss of such SilverSky Equipment regardless of cause. You will pay us for any damaged or unrecoverable SilverSky Equipment. You authorize us and our authorized agents, contractors, representatives, and vendors to enter your premises, with reasonable notice, during normal business hours (or as otherwise authorized by you), to install, maintain, repair, and/or remove any SilverSky Equipment and/or to perform the Security Device Management Services. You must return SilverSky Equipment, at your expense, within 14 days after this Attachment terminates or expires. SilverSky Equipment must be returned in the same condition in which it was provided to you, except for normal wear and tear. If you fail to do so, billing for Security Device Management Services will resume and continue until all SilverSky Equipment is returned. Equipment for Security Device Management Services delivered through us is maintained in a lockdown configuration that does not allow customer administrative access.

5. 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 the use of the Services.

SERVICE LEVEL AGREEMENT FOR

SECURITY DEVICE MANAGEMENT SERVICES

If we fail to meet the levels defined in this Security Device Management 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 Security Device Management 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 on a 24 x 7 x 365 basis. You may reach an individual in each of these departments by calling the appropriate support service.

2. **RESPONSE TIME.** We commit to certain incident response times. These commitments are subject to your providing us 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.

2.1. **Security and Network Operations Events.** We classify all events as high, medium, or low level. We will identify or begin analysis of high level events within fifteen (15) minutes, medium level events within one (1) hour, and low level events within twenty-four (24) hours of occurrence. Failure to respond in accordance with these guidelines will entitle you to a one-day Tier 1 credit for high level events or one-day Tier 2 credit for medium and low level events.

2.2. **Change Requests.** We will make commercially reasonable efforts to begin implementation of changes you request to your service or equipment within twenty-four (24) hours of receipt of the appropriate change control form, requested changes will normally be implemented during Customer's non-business hours. Failure to respond in accordance with these guidelines will entitle you to a one-day Tier 2 credit.

3. **SERVICE AVAILABILITY GUARANTEE.** Our commitment is to have the Services available 99.5% of the time and as set forth below. At your request, we will calculate the number of minutes the Service(s) were not available to you in a calendar month (**"Service Unavailability")**. Service Unavailability will not include unavailability continuing for an hour or less or any unavailability that you fail to report to us within five (5) days. Failure to meet the service level described in this Section will entitle you to receive a Tier 1 credit.

4. **MAINTENANCE.** We reserve the following weekly maintenance windows during which you may experience periodic service outages:

(i) Tuesday and Thursday (12 AM – 2 AM ET)

(ii) Saturday (12 AM – 5 AM ET)

In the event we must perform maintenance during a time other than the service windows provided above, we will provide notification prior to performing the maintenance.

5. **CREDIT REQUEST AND PAYMENT PROCEDURES.** For failures to meet service levels herein in a calendar month, you will be entitled to receive a credit as specified below:

(i) **Tier 1.** Equal to twice the prorated portion of the monthly fee for the affected service; or

(ii) **Tier 2.** Equal to the prorated portion of the monthly fee for the affected service;

provided however that a breach of this SLA due to Exceptions described below will not qualify for such credits.

To receive a credit under this SLA, you must be current with your payments at the time Service Unavailability occurred. In addition, all credit requests must be submitted in writing, either through our ticketing system, via email or fax, or by certified U.S. mail, postage prepaid. You must submit each request for credit within seven (7) days of the occurrence giving rise to the credit claim. 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 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.)

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

(i) Maintenance, as defined above;

(ii) Fiber cuts or other such issues related to telephone company circuits or local ISP outside of our control;

(iii) Your applications, equipment, or facilities;

(iv) You or any of your end-user' acts or omissions;

(v) Reasons of Force Majeure as defined in the MSA;

(vi) Any act or omission on the part of any third party, not reasonably within our control;

(vii) First month of service for the specific Services for which a credit is claimed;

(viii) DNS issues outside our direct control;

(ix) Broadband connectivity.