



SERVICE ATTACHMENT

VULNERABILITY MANAGEMENT “INSIGHT” SERVICES

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

1. **Vulnerability Management Insight Services** (“Insight Services”) will mean SilverSky services, including vulnerability assessments, remediation data reporting of your environment, and automated and recurring vulnerability and compliance scanning of internal, external, and cloud-based live IP addresses. Service SKUs:
 - S-200-3143 SilverSky Insight - User
 - S-200-3144 SilverSky Insight - Server
 - I-200-3143 Installation of SilverSky Insight - User
 - I-200-3144 Installation of SilverSky Insight - Server

2. **Customer Responsibilities.** During the performance of the Insight Services, you agree to perform the following obligations and acknowledge and agree that SilverSky’s ability to perform its obligations and its liability 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 Insight Services;
 - a. Ensure complete and current contact information is provided on a timely basis;
 - b. Contact SilverSky 24/7 support (via email or telephone) to ask questions
 - c. Acknowledge and agree that scanning IP addresses and/or domain names may expose vulnerabilities and, in some circumstances, could result in the disruption of Services or corruption or loss of data.
 - d. Perform regular backups of all data contained in or available through the devices connected to your IP address and/or domain names.
 - e. Acknowledge that the IP address of cloud-based assets is subject to change.
 - f. Identify the specific IP addresses of assets to be scanned.
 - g. Acknowledge that the average monthly number of IP addresses to be scanned does not exceed two (2) IPs per user/server count. If scanned IPs exceed this threshold, SilverSky may increase the number of users/servers charged to better reflect your actual usage.
 - II. You may use the Services only to scan the IP Addresses owned by and registered to Customer, or for which Customer otherwise has the full right, power, and authority to consent to have the Services scan and/or map.
 - a. Scans of external IPs are conducted remotely.
 - b. Scans of internal and cloud-based IPs are conducted from one or more ISO images placed on the Customer’s network or in the Customer’s leased virtual data center. The IP level is based on the Customer’s technical scanning requirements.
 - a. You will not rent, lease, or loan the Services, or any part thereof, or permit third parties to benefit from the use or functionality of the Service via timesharing, service bureau arrangements or otherwise.
 - b. In the event one (1) or more of the IP Addresses identified by You are associated with computer systems that are owned, managed, and/or hosted by a third-party service provider (“Host”), You warrant that you have the consent and authorization from such Host(s) necessary for SilverSky to perform the Services.
 - c. You agree to facilitate any necessary communications and exchanges of information between SilverSky and Host.
 - III. Self-service vulnerability scanning:
 - I. Conduct scanning of your infrastructure from insight.silversky.com
 - i. Scanning may be conducted as an ‘internal’ scan within your network utilizing either agent-based or agentless scanning options or as an ‘external’ scan utilizing the portal.
 - ii. External scans can only be conducted on network assets and infrastructure with an internet-facing external IP address.
 - II. Review vulnerability reports.
 - i. Note: Report capabilities are restricted to the platform’s capabilities and are the Customer’s responsibility to generate. The portal may only be accessed by the named individuals you specify.
 - III. Remediation Plan: Creation of a remediation plan, schedule, and actions to remediate vulnerabilities are the Customer’s responsibility.

3. **SilverSky Responsibility:**
 - I. Company Profile Set-Up. [Insight.Silversky.com](https://insight.silversky.com)
 - II. Service Implementation with authorized users based on your requirements
 - IV. Provide 24/7 email or telephone support for:



- a. Technical issues with the scanner operation or troubleshooting, which will result in a ticket to the SOC team.
 - b. Changing contact information.
 - c. Solving issues associated with accessing the Insight service.
- III. NOTE: Help desk calls cannot be used for general consulting advice that does not directly pertain to the results of the Service
4. **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.



SERVICE LEVEL AGREEMENT FOR INSIGHT SERVICES

We are committed to providing a scalable and highly available messaging solution through the following service commitment (“**Service Level Agreement**”). We will have the Services Available calculated by the following equation:

$$\text{Availability} = \text{Total Monthly Minutes} - \text{Maintenance Minutes} - \text{Downtime Minutes}$$

Defined Terms. For the purposes of this Service Level Agreement, the following terms shall have the following meanings:

“**Available**” or “**Availability**” means that the Insight portal is operational.

“**Downtime Minutes**” means the total number of minutes the Insight portal is not available.

“**Total Monthly Minutes**” means the number of days in the month multiplied by 1,440 minutes per day.

Maintenance Notices. We will communicate the date and time that we intend to make the Services un-Available through a global “welcome message” or an email sent to your Administrator at least 48 hours in advance or longer if practical. You understand and agree that there may be instances where we need to interrupt the Services without notice in order to protect the integrity of the Services due to security issues, virus attacks, spam issues or other unforeseen circumstances.

Measurement. We use a proprietary system to measure whether the Services are Available and you agree that this system will be the sole basis for resolution of any dispute that may arise between you and us regarding this Service Level Agreement.

Service Level Metrics.

Availability. The Service level metric for Availability is 99.999% measured on a monthly basis.

Amount of Service Level Credits.

Availability.

Availability	Amount of Credit for Affected Month
> 99.9% but < 99.999%	5%
> 96.9% but < 99.9%	7%
> 96.9% but < 97.9%	9%
< 96.9%	11%

Remedy and Procedure. Your sole remedy and the procedure for obtaining your remedy in the event that we fail to meet the Service level metrics set forth above are as follows:

You must notify us in writing at support@silversky.com of both the date the Downtime Minutes occurred and an estimate of the amount of actual Downtime Minutes within five business days of the Downtime Minutes (the “**Claim Notice**”). We will confirm the information provided in the Claim Notice within five business days of receipt of the Claim Notice. If we cannot confirm the Downtime Minutes, then you and we agree to refer the matter to executives at each company for resolution. If we confirm that we are out of compliance with this Service Level Agreement, you will receive the amount of Service Level Credits set forth above for the affected Service level metric and the affected Seats for the affected month, that will be reflected in our invoice to you in the month following our confirmation of the Downtime Minutes.

Except as expressly set forth herein, any remedy you may receive pursuant to this section does not relieve you, or allow a set-off, of any other payment obligations to us under this or any other Attachment.