SERVICE OVERVIEW

SilverSky Managed Defender M365

SilverSky is an award-winning cybersecurity industry leader with over 20 years of experience protecting businesses large and small. Our 4,000 customers, with an average tenure of 8 years, count on SilverSky to deliver services and act as an extension of their security team. SilverSky customers improve their security risk posture because of our flexible approach and skilled team members who focus on the mission of safeguarding our customers.

SilverSky offers a Managed Defender M365 solution for our customers who have made an investment in the Microsoft Defender M365 licenses. This solution provides configuration, management, and monitoring of the four security solutions within M365:

1. **Microsoft Defender XDR** - Protect your organization against sophisticated attacks such as phishing and zero-day malware.
2. **Microsoft Defender for Endpoint** - Scale your security with a unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and automated/manual response.
3. **Microsoft Defender for Cloud Apps** - View apps used in your organization, identify and combat cyber threats, and monitor and control data travel in real-time.
4. **Microsoft Defender for Identity** - Use a cloud-based solution to protect your organization’s identities from multiple types of advanced targeted cyberattacks.

SilverSky Managed Defender M365 is part of the Lightning platform, which evolved from our strong Managed Security Services heritage coupled with the addition of military-grade data analytics. Our approach proudly puts the “R” in MDR (Managed Detection & Response) with a recognition that a successful response will show customers receive fewer alerts over time. SilverSky backs the Managed Defender M365 service with a ten-minute notification SLA on critical alerts.

SilverSky Managed Defender M365 makes the most of your investment in Microsoft licensing by tuning the environment to meet your business objectives and monitoring the telemetry from these services to respond to security activity. Silversky has been a Microsoft partner for over 15 years, earning the important distinction of a Solutions Designation Partner. We hold dozens of Microsoft certifications and stay on top of the myriad of changes Microsoft makes to its licensing and feature set on an annual basis. This expertise provides our customers with a tailored solution that evolves over time as both the product features mature and the customer's business changes.

Once configured, each product triggers security alerts based on activity across the customer environment. Alert impact scores are analyzed through our global Security Operations Center (“SOC”), with skilled analysts responding to critical issues 24x7. SilverSky is built on a foundation of compliance, with a rigorous security controls program that includes continuous internal and external audits.

Key Benefits

- Utilizes your investment in Microsoft security and cloud technologies.
- Configuration, ongoing management, and tuning of the four products within Defender M365.
- Global 24x7x365 SOC provides detection and response, enabling security teams to maximize productivity and effectiveness.
- Fast, actionable guidance to address threats before they cause damage to your business.
- Response plans tailored to your business, with real-time insights into security activity, audit trails, and full alert transparency.
- Reduces the time to threat detection with greater fidelity and actionable insights, presenting only relevant alerts to the SOC analyst to speed review and resolution.
- Provides situational awareness across the continuously changing threat landscape.
- Allows you to maximize your investment in Microsoft Defender's security stack while reducing resource skill shortages and preventing technology cost creep.

Key Features

- SOC-as-a-Service – an extension of your own security and IT staff providing continuous 24x7 monitoring of your security environment.
- Configure and deploy up to four Microsoft Defender applications
- Customer portal – View and audit the alert response process with integrated dashboards, incident management, and flexible reporting.

Customized Response Through SilverSky Playbooks

SilverSky works with our customers to create customized playbooks to match their business needs, available technical resources, and incident response plans. These playbooks define the customer's notification preference based on incident criticality. Playbooks can be updated at any time, with full audit tracking, and once submitted, will take effect in real time. Playbooks can be grouped by devices, flexibly matching the customer's business requirements.

Service Overview

SilverSky Managed Defender M365 consists of SilverSky configuring, managing, and monitoring the customer-owned Microsoft Defender M365 services. It provides near real-time security event analysis across the customer's security and critical infrastructure 24/7. The customer is responsible for any license and consumption fees for the customer's environment. SilverSky and the customer will have access to the Microsoft XDR portal provided by the customer.

Management activities include service implementation, configuration changes necessary for successfully provisioning the Managed Defender M365 and tuning the four M365 products for cybersecurity efficiency and cost optimization.

Our highly skilled and certified team of Microsoft experts manage the individual products, responding to alerts and sharing the results in our Lighting customer portal. The customer portal provides a single view into all of the security activity across the Microsoft Defender M365 products, with log detail, analyst comments, and tailored reporting available. Our noise reduction approach minimizes the need to hunt through alerts: this dramatically reduces human error and effort. This approach allows our analysts to focus on a small number of impactful alerts to your business, notifying you according to your personalized response playbook and reducing alert fatigue.

How It Works

SilverSky will provide the customer with the following services:

- Defender M365 services: Microsoft Defender XDR, Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, and Microsoft Defender for Identity
- We will advise and support customers installing these tools on endpoints, including servers, workstations, and laptops.
- An agent can be deployed on each endpoint the customer identifies needing the service.
- We will advise and support customers in installing agents on their endpoints, but the customer performs the installation.
- Data is processed within the customer-provided Microsoft XDR portal by alerting our SOC through the customer portal.
- Customer portal analytics reduce false positives.
- Security event detection and prioritization as per our service level agreement.
- Automated monthly reporting.
- Analysts will review, analyze, and document their findings in our Lightning platform.
- Severity of the event triggers customer notification following the customer playbook response plan.
- Tailored reporting and a full audit trail are available in the customer portal.

Proactive Service Support Hours

SilverSky Managed Defender M365 includes up to twenty proactive service support hours annually. These Hours can be utilized for the ongoing management of the in-scope Microsoft Defender M365 technologies, the configuration of custom source ingestion, or specialized Microsoft Defender M365 engagements. Proactive service support ensures that SilverSky is there to help secure every step of your IT journey, regardless of whether you completed deployment last week or last year.

Service	Deliverable
Installation	SilverSky will assist the customer with the deployment of Defender M365, licensed by the customer. The customer is responsible for: • Designating a primary point of contact who will be available to assist SilverSky with installation is an appropriately qualified and trained technical lead who will be a permanent stakeholder throughout the engagement. • Providing information about the organization's software inventory, critical assets, and VIP users. • Deploying agents and adjusting network settings as directed by SilverSky and Microsoft; responsible for the quality of data and any remediation efforts that may be necessary to complete service implementation. • Decisions made regarding this service implementation. • Completing any direct or physical remediation. • Co-managing the customer-provided Microsoft XDR portal
Policy Tuning	SilverSky will respond to policy tuning and update requests based on customer-identified priorities. • Adding or removing exceptions • Modifying automated response policies • Tuning alert notification rules
Alert Monitoring	Defender M365 alerts will be monitored 24/7 in the customer portal platform and tracked through a three-stage process. Triage Alarms: Incoming alerts from Microsoft Defender M365 are categorized by severity, grouped with associated events, and may be resolved if certain criteria are met. Incidents are created when the alerts cannot be resolved without further analysis. Analyze & Conclude: A SOC analyst reviews the incident**, gathers additional context, and may escalate to upper levels of the SOC organization as needed. A conclusion is reached when the analyst(s) decide to resolve the incident as benign, escalate the incident to the customer, or act to quarantine/un-quarantine an endpoint based on the analysis. Escalate & Assist: The SOC will escalate incidents to the customer if additional information is required or if there is a potential security breach. In the event of a potential breach, the SilverSky analyst will provide guidance on the next steps for investigation or remediation. SilverSky does not provide remediation activities for this service and may recommend the use of a 3rd-party incident response team.

	**Depending on the severity level, it may be aggregated in the customer portal and performed as a multi-alert review.
Product Support	SilverSky will respond to product support requests based on priority. We will handle L1 support and may escalate to the Microsoft support team for L2/L3 support.
Reporting	SilverSky will provide initial training and training materials for the customer portal. The Report Builder feature in the customer portal allows users to create additional reports.

Moving from Implementation to Operations

SilverSky defines a completed Managed Defender M365 service deployment as the date when the following steps have been completed:

1) All Microsoft Lighthouse and GDAP delegations are functional.
2) Defender Configuration deployed.
3) Alerts are ingested from configured Defender sources and validated by SilverSky SOC.
4) SOC Playbooks approved.
5) Customer onboarded to Lightning Customer Portal.

Any changes requested after that date will be managed through our service operations, customer portal service tickets or customer support team.

RACI Matrix

Roles and Responsibilities are used to assign the level of task responsibility for various components of the SilverSky services:

Responsible	The person who is responsible for doing the work
Accountable	The person who is ultimately accountable for the process or task being completed properly
Consulted	People who are not directly involved with carrying out the task but who are informed
Informed	Those who receive output from the process or task or have a need to stay in the know

Task ownership for the Managed M365 service:

Activity	**SilverSky**	**Customer**
Participation in deployment project kickoff and ongoing service-related meetings	AC	IR
Enable and configure logging on remote systems or devices per SilverSky instructions	IC	RA
The customer is responsible for charges related to Microsoft licenses and fees payable to Microsoft	IC	RA
Provide a Virtual Machine for a Log Collector Virtual Appliance (document provided) as needed. The log collector is required for onboarding logs from M365 log sources.	IC	RA
Provide remote access for administration of the Log Collector Virtual Appliance	IC	RA

Provide access to an internal Subject Matter Expert (SME) responsible for managing the specific log source type.	IC	RA
Manage log retention & archiving: The customer is responsible for managing the log archiving processes for historical, backup, compliance, regulatory, or other requirements.	IC	RA
Configure all log sources so that logs are appropriately sent to the agents and log collection devices. This includes, but is not limited to, any intermediary log sources. If changes to the customer's existing network architecture are required for Service implementation, SilverSky will communicate these changes to the customer.	IC	RA
Provide detailed information on the network environment to facilitate the deployment of the SilverSky solution. Notify SilverSky of any environmental changes that may affect the execution of the Service.	IC	RA
Install appropriate collecting agents, as per SilverSky instructions.	IC	RA
Co-manage the Microsoft Lighthouse portal	RACI	RACI
Provide feedback on fine-tuning alerts and playbooks when required.	IC	RA
Notify SilverSky of any necessary user account changes tied to customer employee termination; this includes employees or contractors that have access to the SilverSky customer portal or approval to contact the SOC.	IC	RA
Perform additional remediation: During an investigation of security alerts, the SilverSky Security Operation Center may give guidance to a customer to perform specific actions in the customer's environment to improve the customer's security posture or to fully remediate an incident. The performance of these actions is the customer's responsibility.	IC	RA
Obfuscate Personally Identifiable Information (PII) data in the customer's environment. SilverSky will not extract personally identifiable information from the Partner or customer environment or store it within the SilverSky environment except for only the sufficient log data for enrichment, case management, reporting, and automation purposes. No raw or PII data should leave the customer's M365 environment.	IC	RA
The customer is responsible for providing and maintaining API credentials for SilverSky when required.	IC	RA
Technical resource with an understanding of customer's security policies, network configuration and service requirements to assist with service implementation and participation in testing. Provide timely access to project stakeholders to support the objectives of the Managed Defender M365 service.	IC	RA
Provide internet access and manage firewall rules when required.	IC	RA
Defining the actions that SOC analysts will take based on incident criticality in the SilverSky customized playbooks	IC	RA
Create and manage case and incident tickets following the SilverSky playbooks	RA	IC
Security alert monitoring 24x7	RA	IC

Global SOC staffed with skilled Level 1, 2 and 3 analysts	RA	IC
Interacting with SOC analysts, viewing and responding to incident tickets via the customer portal	IC	RA
Provide robust and flexible reporting including historical views, active tickets, audit trail, compliance reporting with scheduled and on-demand reporting	RA	IC
Provide a file repository for saved reports and asset information	RA	IC
Training on customer portal & reporting	RA	IC
Alert handling, severity scoring with response recommendations	RC	IA
10-minute Service Level Agreement (SLA) to identify a critical alert	RA	IC
Provide 24x7 support of the Lightning platform and customer portal	RA	IC