SilverSky Managed Endpoint Detection and Response

SilverSky protects thousands of organizations from cyber attacks and has done so for over 20 years. Our experience in providing 24x7 Security Operations Center (SOC) services, numerous industry certifications, deep technology insights, and an appreciation for working collaboratively with our customer's security teams make us an ideal partner to assist in protecting edge devices.

SilverSky has developed a managed endpoint security service in partnership with SentinelOne that addresses the challenges of preventing, detecting, and responding to known and unknown attacks. Our MEDR (Managed Endpoint Detection and Response) service includes SentinelOne Singularity Complete Agent licenses.

Key Benefits

- Improved security posture – Take advantage of SentinelOne's patented AI algorithms to detect a wide array of threats, plus self-healing response capabilities that reverse malicious activity in real-time.
- Skilled cybersecurity team – Our team of cybersecurity experts work with you for efficient installation and system tuning. You get time back to focus on other priorities.
- Maximize ROI—SilverSky's affordable MEDR provides deployment guidance and support services to ensure you get the most from your investment.

Combining best-of-breed Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) with a 24/7 SOC, SilverSky helps you to proactively eliminate threats and meet compliance objectives.

Key Features

- SOC-as-a-Service – an extension of your security and IT staff providing continuous 24x7 monitoring of your security environment.
- Configure & Deploy SentinelOne – Best-of-breed EPP and EDR are configured and deployed by SilverSky Solutions Engineers and Security Analysts. The SOC is available to assist with agent rollout guidance, but the installation of the agents across a customer estate principally lies with the customer.
- Customer portal – View and audit the alert response process with integrated dashboards, incident management, and flexible reporting.

How It Works

SilverSky will provide the customer with the following services:

- SentinelOne Agents are installed on customer endpoints, including servers, workstations, and laptops.
    - An agent can be deployed on each endpoint that the customer identifies as needing the service.
    - We will advise and support customers in their installation on customer endpoints. However, the installation of SentinelOne Agents is performed by the customer.
- Data is processed by the SentinelOne Cloud with alerting to our SOC through the customer portal
- Customer portal analytics reduce false positives
- Security event detection and prioritization as per the SLA
- Automated monthly reporting

Service	Deliverable
Installation	SilverSky will assist the customer with the deployment of SentinelOne endpoints licensed through SilverSky. 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 SentinelOne; responsible for the quality of data and any remediation efforts that may be necessary to complete service implementation. • The authority and responsibility for decisions made regarding this service implementation. • The responsibility for any direct or physical remediation.
Policy Tuning	SilverSky will respond to policy tuning and update requests based on priority. • Adding or removing exceptions • Modifying automated response policies • Tuning alert notification rules

Alert Monitoring	SentinelOne alerts will be monitored around the clock in the customer portal platform and tracked through a three-stage process. Triage Alarms: Incoming alerts from SentinelOne are categorized by severity and grouped with associated events. They may be resolved if specific 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 in this service level and may recommend the use of a 3rd-party incident response team. **May be aggregated in the customer portal and performed as a multi-alert review depending on severity level.
Product Support	SilverSky will respond to product support requests based on priority. SilverSky will be responsible for handling L1 support and may escalate to the SentinelOne support team for L2 support.
Reporting	SilverSky will provide initial training and training materials for the customer portal. Members of the SilverSky Account Management team will assist with configuring reports, including format and scheduling security alerts. The system or the customer portal do not generate specific reports regarding this service.

Service Deployment

SilverSky defines a completed MEDR service deployment as the date when the following steps have been completed:

(1) Pilot phase completed and customer has approved moving to a full Protect-Protect mode for at least one Group.
(2) The customer knows how to deploy the agents.
(3) Portal training (on SentinelOne portal and Lightning Customer Portal) has been completed.

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 SilverSky Managed Endpoint Detection and Response service:

Activity	SilverSky	Customer
Solution evaluation	RA	CIR
Participation in kickoff and quarterly meetings	AC	IR
Training on initial agent deployment & troubleshooting	RA	IC
SentinelOne agent installation on customers' endpoints	IC	RA
Technical resource with an understanding of Customer's security policies, network configuration and service requirements to assist with service implementation & participation in testing	IC	RA
Direct or physical remediation of endpoints	IC	RA
Alert monitoring	RA	IC
Reporting on security alerts in Lightning managed console	RA	IC
Remediation or investigation guidance to support customer resolution	RA	IC
Training and orientation on SentinelOne portal	RA	IC
Agent update scheduling & coordination	RA	IC
Ensure that agent updates are successful on endpoints	IC	RA
Management of agent groups	RA	IC
Post-incident analysis & agent tuning/exclusion	RC	IA
Provide 24x7 support of the Lightning platform and manage ongoing support issues of SentinelOne portal	RA	IC